

IN THE UNITED STATES DISTRICT COURT

FOR THE SOUTHERN DISTRICT OF NEW YORK

JASON GOODMAN

Plaintiff,

vs.

CHRISTOPHER ELLIS BOUZY, BOT  
SENTINEL, INC, GEORGE WEBB  
SWEIGERT, DAVID GEORGE SWEIGERT,  
BENJAMIN WITTES, NINA JANKOWICZ,  
ADAM SHARP, MARGARET ESQUENET,  
THE ACADEMY OF TELEVISION ARTS  
AND SCIENCES, SETH BERLIN,  
MAXWELL MISHKIN, RICHARD LOURY

Defendants

Case No.: 1:21-cv-10878-AT-JLC

**PROPOSED THIRD AMENDED  
COMPLAINT FOR FRAUD,  
DEFAMATION, ABUSE OF PROCESS,  
CIVIL CONSPIRACY, AND  
RACKETEERING**

**JURY TRIAL DEMANDED**

Pro Se plaintiff Jason Goodman (“Goodman”) respectfully submits this third amended complaint in response to Magistrate Judge Judge James L. Cott’s order (ECF No. 134) and pursuant to Judge Torres’ Individual Practices in Civil Cases Rule III. B. iv., FRCP Rule 15(a)(1)(B), and in response to defendants’ motions to dismiss (ECF Nos. 106 and 112). Goodman alleges as follows, upon actual knowledge with respect to himself and his own acts, and upon information and belief as to all other matters.

**PRELIMINARY STATEMENT**

In January 2014, defendant David George Sweigert (“Sweigert”) published a cyber security white paper titled “Expanding the Role of National Guard Cyber Units to Support Disaster Response and recovery and make a Cyber Militia a Reality”. **(EXHIBIT A)**

PROPOSED THIRD AMENDED COMPLAINT FOR FRAUD, DEFAMATION, ABUSE OF  
PROCESS, CIVIL CONSPIRACY, AND RACKETEERING- 1

1 As the document demonstrates, Sweigert had cyber warfare in mind years before  
2 Goodman encountered him or interacted with his brother George Webb Sweigert (“Webb”).  
3 Sweigert published a series of 254 papers starting in approximate 2013 that closely track trends  
4 in the cyber security industry (<https://www.slideshare.net/dgsweigert/presentations>). Sweigert  
5 systematically sent many of those papers to Senators, Governors, Attorneys General, the Coast  
6 Guard, the Department of Homeland Security, and others just as a professional in the field  
7 seeking to keep himself relevant and available for government contracts would. Sweigert has  
8 publicly boasted about his background as a contractor to various U.S. government agencies and  
9 his experience in the U.S. Air Force. After a June 14, 2017 incident in Charleston, SC resulting  
10 in the closure of the port ([https://www.nytimes.com/2017/06/15/us/port-dirty-bomb-south-](https://www.nytimes.com/2017/06/15/us/port-dirty-bomb-south-carolina.html)  
11 [carolina.html](https://www.nytimes.com/2017/06/15/us/port-dirty-bomb-south-carolina.html)), Sweigert published a video announcing the immediately urgent need for a “Cyber  
12 Militia”. In it, Sweigert declared, “we’re moving fast because I’m working around waiting for  
13 consensus from government people or industry people or people like that. We’re moving ahead  
14 with the actual scenario that’s going to be used by actual infrastructure operators. I guarantee you  
15 what we’re doing right now is going to be documented and it’s going to be read by several dozen  
16 key people that run the critical infrastructure of the United States.”  
17 ([https://vk.com/video731682021\\_456239025](https://vk.com/video731682021_456239025))  
18

19 It is unclear how Sweigert could make such guarantees or who exactly he was addressing  
20 in the video, but on information and belief, Goodman alleged Sweigert was attempting to  
21 insinuate himself into the community that would become the Department of Homeland Security  
22 (“DHS”) Disinformation Governance Board (“DGB”). Sweigert’s video is an  
23 uncharacteristically concise and clear lecture informing viewers about the history and purpose of  
24  
25  
26  
27

1 cyber militias around the world in countries including Lithuania. Referring to the June 14, 2017  
2 Port of Charleston closure, Sweigert goes on to say “And this incident that happened with  
3 George is a perfect example to start dusting some of these things off and seeing if they work.  
4 Especially in the cyber militia concept. We can't talk about this stuff anymore. It's time for  
5 action.” The full transcript of the video reveals more details of Sweigert’s plans. **(EXHIBIT B)**

7 Joseph L. Lengyel was the Chief of the National Guard Bureau in 2017. The  
8 General had rightful legal authority over the National Guard and its various units. He could have  
9 conceivably stood up a cyber militia or otherwise gone through the procedure of legally creating  
10 one, but Sweigert had no such legal authority. Despite this, and based on his own public  
11 statements, Goodman alleges Sweigert calculated a plan to illegally form his own Cyber Militia  
12 staff it with cyber vigilantes and point it at Goodman. After publishing his video, Sweigert also  
13 published a book in violation of 18 U.S. Code §§ 1343, 1513, 1951 and 1962(b) entitled “Report:  
14 The Port of Charleston Dirty Bomb Hoax and Social Media Liability” which is available to buy  
15 on Amazon.com (/1717056792/ref=cm\_cr\_arp\_d\_product\_top?ie=UTF8) **(EXHIBIT C)**

18 Sweigert’s book falsely claims Goodman planned a bomb hoax intended to shut the port  
19 of Charleston using DDoS and other cyber hacking techniques Goodman has no knowledge of  
20 for the alleged purpose of boosting YouTube viewership. The allegations are unfounded and  
21 false, but Sweigert has focused on Goodman since 2017, attempting to demonstrate that  
22 Goodman engaged in these and other crimes including terrorism, rape, and the spread of  
23 disinformation. Sweigert enlisted the help of defendants and engaged in a coordinated array of  
24 predicate acts in a pattern calculated to harm Goodman and his business and to deprive him of  
25 property in a continuous and ongoing manner. Sweigert’s Cyber Militia is not a corporation,  
26  
27

28 PROPOSED THIRD AMENDED COMPLAINT FOR FRAUD, DEFAMATION, ABUSE OF  
PROCESS, CIVIL CONSPIRACY, AND RACKETEERING- 3

1 legal partnership, or government agency. It is an association in fact enterprise (the “Enterprise”)  
2 illegally created by him. It is a vigilante internet “hit squad” that he has set upon Goodman.

3 Defendant Nina Jankowicz (“Jankowicz”) publicly announced her employment as  
4 Executive Director of the DGB on or around April 27, 2022. It was first published in Politico by  
5 Daniel Lippman, later confirmed. (<https://twitter.com/wiczipedia/status/1519274470049042432>)  
6

7 During a May 4, 2022 hearing, Senator Josh Hawley, R-MO (“Hawley”) revealed that a  
8 DHS whistleblower had turned over documents including the DHS DGB Charter and related  
9 documentation. **(EXHIBIT D)**  
10

11 Previously classified documents included with the whistleblower release reveal that the  
12 DGB refers to mis- dis- and mal-information as (“MDM”). The document does not describe any  
13 process by which the DGB determines the veracity of any given item of information, but it  
14 mentions “Procurement guidelines for contracting with third parties to support the Department's  
15 MDM efforts;”. Goodman alleges Jankowicz or others within DHS have contracted with  
16 Sweigert to provide support for MDM mitigation through some unspecified means. Through the  
17 Enterprise, Sweigert has engaged in activity outside of legal actions described by the DHS that  
18 violate 18 U.S. Code §1962(b) and other statutes as described herein.  
19

20 Defendant Benjamin Wittes (“Wittes”) is the editor of the Lawfare Blog  
21 ([www.lawfareblog.com](http://www.lawfareblog.com)). Wittes own blog defines the term lawfare as “the use of law as a  
22 weapon of conflict”. (<https://www.lawfareblog.com/about-lawfare-brief-history-term-and-site>).  
23 More broadly, lawfare is generally regarded as the weaponization of the legal system against an  
24 enemy and masking the attack as legitimate litigation. This is precisely what Goodman alleges  
25 defendants in this case have done by and through their collaboration in the Enterprise.  
26  
27

28 PROPOSED THIRD AMENDED COMPLAINT FOR FRAUD, DEFAMATION, ABUSE OF  
PROCESS, CIVIL CONSPIRACY, AND RACKETEERING- 4

1 Lawfare is the primary weapon of the Enterprise. Sweigert, with the help of defendants  
2 has endeavored to overwhelm Goodman with vexatious legal action and numerous fraudulent  
3 police reports. These vexatious legal actions in and of themselves demonstrate a pattern of  
4 related activity. Additionally, Sweigert has written countless emails and other communications  
5 to Goodman and his associates including extorting attorney Jonathan Snyder (“Snyder”) into  
6 withdrawing from representing Goodman’s company in prior litigation and to deny Goodman’s  
7 right to a fair trial and due process. These malicious acts aimed to destroy Goodman’s business  
8 relationships, his ability to conduct commerce online, prevent him from engaging in journalism  
9 and his terminating his access to social media.  
10  
11

#### 12 **CIVIL RICO STANDING AND JURISDICTION**

13 Section 1965(b) of the RICO statute provides for national jurisdiction over “additional  
14 defendants of any kind,” but only if the plaintiff shows “that the ‘ends of justice’ so require.” PT  
15 United Can Co. v. Crown Cork & Seal Co., 138 F.3d 65, 71 (2d Cir. 1998). Generally, “‘ends of  
16 justice’ jurisdiction is authorized where the RICO claim could not otherwise be tried in a single  
17 action because no district court could exercise personal jurisdiction over all of the defendants.”  
18 Elsevier Inc. v. W.H.P.R., Inc., 692 F. Supp. 2d 297, 315 (S.D.N.Y. 2010) (citations omitted). To  
19 comply with due process, any such additional defendant need only have minimum contacts with  
20 the United States. See Hitachi Data Sys. Credit Corp. v. Precision Discovery, Inc., 331 F. Supp.  
21 3d 130, 145 (S.D.N.Y. 2018) “If these requirements are satisfied, the Court may also be  
22 permitted to exercise personal jurisdiction over such defendants for other claims that arise out of  
23 the same operative facts as the civil RICO claim, even if personal jurisdiction would not  
24 otherwise be present as to those claims.” Id. (citing IUE AFL-CIO Pension Fund v. Herrmann, 9  
25  
26  
27

1 F.3d 1049, 1056–57 (2d Cir. 1993)). Defendants attempt to disparage Goodman’s claims by  
2 referring to them as a “fraudulent conspiracy” theory. Evidence presented herein will prove an  
3 actual conspiracy carried out by defendants by and through participation in the Enterprise.  
4

#### 5 **FACTUAL ALLEGATIONS**

- 6 1. Defendant Sweigert is a culpable person in this case, who maintains control over an  
7 “Enterprise” affecting interstate commerce through a “pattern” of “racketeering  
8 activity.” Plaintiff Goodman has been and continues to be injured “by reason of”  
9 Sweigert’s RICO activity and that of his co-defendants in a continuous, ongoing  
10 manner as explained below.  
11
- 12 2. Defendants’ pattern of racketeering activity is continuous and comprised of related  
13 predicate acts that represents an open-ended scheme which not only poses a threat of  
14 continuity but is continuous today. Defendants regularly engage in conduct that by  
15 its nature projects into the future and poses an ongoing threat of repetition.  
16
- 17 3. Defendants participated in an association in fact enterprise which Sweigert has  
18 referred to as a Cyber Militia (the “Enterprise” or “Cyber Militia”) and worked  
19 together toward a common purpose through a pattern of racketeering activity with the  
20 common goal to harm Goodman’s business and deprive him of access to property and  
21 constitutional rights.  
22
- 23 4. Sweigert acquired control over the Enterprise by forming his own private cyber army  
24 illegally, not through the proper channels of joining the National Guard or otherwise  
25 being granted official government authority to do so.  
26  
27

- 1       5. In furtherance of the collective purpose of the Enterprise, Sweigert published a book  
2       on April 14, 2018, entitled “Report: The Port of Charleston Dirty Bomb Hoax and  
3       Social Media Liability” in violation of 18 U.S. Code §§ 1343 and 1513 containing  
4       known false allegations of terrorism committed by Goodman.  
5
- 6       6. The Enterprise receives income from this book in violation of 18 U.S. Code § 1962.  
7
- 8       7. Sweigert used false allegations in his book to support vexatious litigation he filed  
9       against Goodman in the U.S. District Court for the District of South Carolina (*See*  
10       *Sweigert v Goodman 2:18-cv-01633-RMG ECF No. 1*) and again in vexatious efforts  
11       to intervene in existing litigation against Goodman in the Eastern District of Virginia  
12       brought by non-party Robert David Steele (“RDS”) an associate of Webb, who was  
13       introduced to Goodman by Webb one day prior to the events in the Port of  
14       Charleston. (*See Steele et al v Goodman et al Case 3:17-cv-00601-MHL ECF No. 73*)  
15
- 16       8. Defendants worked with a common purpose, to overwhelm Goodman legally and  
17       financially, toward a common goal of removing Goodman’s ability to do commerce  
18       and conduct business online, to extort Goodman into terminating broadcasts of factual  
19       first amendment protected statements and opinions unfavorable to defendants, and  
20       with continuity for more than five years, up to and including today in an ongoing and  
21       continuous manner, violating 18 U.S. Code § 1962(b)(c) and (d).  
22
- 23       9. Sweigert brought defendants Sharp, Esquenet and ATAS into the Enterprise with a  
24       fraudulent email sent on or around June 28, 2020 that included false statements  
25       alleging Goodman had violated ATAS copyright and that the author’s grandmother  
26       had died in violation of 18 U.S. Code §§ 1343 and 1513. The claims were intended to  
27

1 incite ATAS to sue Goodman's corporation and to provide Sweigert an advantage in  
2 other existing litigation against Goodman. **(EXHIBIT E)**

3 10. In or around June 2020, simultaneous with the fraudulent email and in further  
4 violation of 18 U.S. Code §§ 1343 and 1513, Sweigert fraudulently communicated to  
5 Sharp, Esquenet and ATAS that Goodman owned a corporation named Multimedia  
6 System Design, INC. D/B/A/ Crowdsource the Truth ("MSDI") with the intention of  
7 inducing defendants to sue MSDI for actions carried out by Goodman unrelated to the  
8 fabricated corporate entity with the specific intent to deny Goodman's right to a fair  
9 trial and opportunity to defend himself pro se.  
10

11 11. Goodman owns a corporation called Multimedia System Design, INC, ("MSD") but it  
12 does not do business as Crowdsource the Truth and has never sought or been granted  
13 the assume name Crowdsource the Truth.  
14

15 12. Goodman hired attorney Snyder to unwind the deliberate confusion because as a non-  
16 attorney, with a corporate defendant named, Goodman had no other option.  
17

18 13. Sweigert threatened and intimidated Snyder with death threats published on the  
19 internet and fraudulent bar complaints, extorting Snyder into withdrawal in violation  
20 of 18 U.S. Code §§ 1343, 1503, 1513 and 1951 and with the express intent of  
21 harming Goodman for the purpose of gaining an unfair advantage in litigation.  
22

23 14. Even after Goodman warned Esquenet, Sharp and ATAS of the existence of the  
24 Enterprise and its motive to draw them in, they chose to proceed "conducting" and  
25 "participating in the conduct of" the affairs of the Enterprise voluntarily cooperating  
26 with Sweigert demonstrating willful intent to commit predicate RICO acts.  
27



1 15. Defendants worked together, sharing information between one another including the  
2 email address [cstt72@protonmail.com](mailto:cstt72@protonmail.com) and other information to harm Goodman.

3 16. Defendants and additional non-parties communicated over the internet, telephones  
4 and by other means, in violation of 18 U.S. Code § 1343 assisting one another across  
5 a range of vexatious legal actions filed in numerous divisions of multiple U.S. District  
6 Courts and General District Court in Arlington VA.

7 17. Goodman, his public reputation, business, property and ability to earn a living were  
8 harmed by the individual predicate acts severally and jointly by the ongoing  
9 racketeering activity of the Enterprise.  
10

11 18. On January 9, 2023, upon learning Goodman would travel to Florida to care for an  
12 elderly family member, with the assistance of Sweigert and in violation of 18 U.S.  
13 Code §§ 1343, 1503, 1513, and 1951, Jankowicz made false statements to law  
14 enforcement in Arlington, VA claiming Goodman had threatened her order to  
15 wrongfully obtain a preliminary order of protection against Goodman. **(EXHIBIT F)**  
16

#### 17 **PARTIES AND NON-PARTIES**

18 19. Plaintiff – pro se Jason Goodman is a New York citizen, an investigative journalist,  
19 documentary filmmaker, talk show host, and founder of the widely trusted news,  
20 information, and entertainment brand Crowdsourcethe Truth. He is separately the  
21 owner of Multimedia System Design, Inc., (“MSD”) a dormant New York  
22 corporation with no employees, no regular revenue, and no ongoing business activity.  
23  
24  
25  
26  
27

1 20. Defendant – Christopher Ellis Bouzy (“Bouzy”) is a New Jersey citizen and CEO of  
2 Bot Sentinel, Inc., which claims to be an artificial intelligence technology company  
3 that identifies and eliminates so called “disinformation” as determined by Bouzy.  
4

5 21. Defendant – Bot Sentinel, Inc., (“Bot Sentinel”) is a New Jersey Corporation that  
6 claims to be an online platform intended to detect and eliminate untrustworthy  
7 internet activity using artificial intelligence and machine learning among other things.

8 22. Defendant – David George Sweigert ("Sweigert") is believed to be a homeless  
9 vagrant, a retired Air Force radio communications and Information Technology  
10 specialist, a professional hacker, the author of the Ethical Hacker’s Field Operations  
11 Guide, a self-proclaimed contractor to the U.S. Department of Homeland Security and  
12 other government agencies, and an aggressive, persistent, vexatious pro se litigant.  
13 Sweigert is the author of the online blog [www.sdney.org](http://www.sdney.org) which purports to engage in  
14 “Disinformation Governance in the Southern District of New York” but is actually a  
15 platform for amplifying false claims against Goodman. **(EXHIBIT A)**  
16

17 23. Defendant – George Webb Sweigert (“Webb”) is a homeless vagrant who currently  
18 claims to be a citizen of Georgia and a journalist. Webb and Sweigert are brothers  
19 (collectively hereinafter “Sweigerts” or “Sweigert Brothers”).  
20

21 24. Defendant Benjamin Wittes (“Wittes”) is a self-proclaimed legal journalist, a Senior  
22 Fellow in Governance Studies at the non-profit think tank the Brookings Institution  
23 and the Editor in Chief of the website [Lawfareblog.com](http://Lawfareblog.com) (“Lawfareblog”).  
24

25 25. Defendant Nina Jankowicz (“Jankowicz”) is the sole proprietor of Sophias Strategies,  
26 LLC, (“Sophias Strategies”) the former Director of the U.S. Department of Homeland  
27

1 Security Disinformation Governance Board (“Disinfo Board”), and a self-proclaimed  
2 expert in so called “disinformation” and Russian internet activity including hacking  
3 and internet “bot” deployment.

4  
5 26. Defendant - Adam Sharp ("Sharp") is the founder and CEO of Sharp Things, LLC,  
6 the President and CEO of the National Academy of Television Arts and Sciences,  
7 (“NATAS”) the former Government Liaison for Twitter, a widely recognized social  
8 media expert, and self-proclaimed “Democrat Political Operative”.

9  
10 27. Defendant – Margaret Esquenet ("Esquenet") is an attorney with Finnegan,  
11 Henderson, Farabow, Garrett & Dunner, LLP (“Finnegan”) who represented  
12 Defendants in prior action against Goodman’s dormant corporation MSD.

13 28. Defendant – The Academy of Television Arts and Sciences ("ATAS" or “Television  
14 Academy”) is one of the key plaintiffs in a vexatious suit wrongfully brought against  
15 Goodman’s dormant corporation MSD for an improper purpose.

16  
17 29. Defendant – Seth Berlin ("Berlin") is an attorney with Ballard Spahr and counsel for  
18 Bouzy and Bot Sentinel in this case.

19 30. Defendant – Maxwell Mishkin ("Miskin") is an attorney with Ballard Spahr and  
20 counsel for Bouzy and Bot Sentinel in this case.

21 31. Defendant Richard Loury ("Loury") is a clerk at the U.S. District Court in the Eastern  
22 District of Michigan ("MIED").

23  
24 32. Non-Party – Robert David Steele (“RDS”) is a self-proclaimed retired Central  
25 Intelligence Agency (“CIA”), employee and the former director of the non-profit

corporation Earth Intelligence Network (“EIN”). RDS was an associate of Webb who reportedly died of Covid-19 in 2021.

33. Non-party – Jonathan Snyder (“Snyder”) is an attorney who formerly represented MSD in litigation with Defendants but withdrew citing harassment by Sweigert.

### **JURISDICTION AND VENUE**

34. This Court has original subject-matter jurisdiction pursuant to 18 U.S.C. § 1964(c) and 28 U.S.C. § 1331 because this action arises under the Federal Racketeer Influenced and Corrupt Organizations Act (“RICO”).

35. This Court also has subject matter jurisdiction pursuant to 28 U.S.C. § 1332 because the amount in controversy exceeds \$75,000, exclusive of interest and costs and there is complete diversity of citizenship between Plaintiff and the Defendants.

36. This Court has jurisdiction over Plaintiff’s related state and common law claims pursuant to the doctrine of supplemental jurisdiction, 28 U.S.C. § 1367.

37. This Court has personal jurisdiction over Defendants under 18 U.S.C. § 1965(b) because pursuant to the RICO statute, an action brought in any U.S. District Court allows that Court to summon parties residing in another district to its own if the “ends of justice require” as is the case in this instant matter.

38. This Court has personal jurisdiction over Defendants because they deliberately directed their conduct at this forum, at Goodman in New York, and at the Court itself.

39. This Court has personal jurisdiction over Bouzy because he directed conduct at this forum when he participated in the Enterprise. The exercise of jurisdiction over Bouzy is reasonable because he conspired with Defendants to destroy Goodman’s business

1 and reputation and terminate his access to social media using Bot Sentinel technology  
2 under his own control with the objective of harming Goodman. This Court has  
3 personal jurisdiction over Bouzy because he participated in a scheme in violation of  
4 18 U.S. Code § 1513(b)(2) to retaliate against Goodman for bringing legal action  
5 against him and Bot Sentinel. This Court also has personal jurisdiction over Bouzy  
6 under 18 U.S. Code § 1965(b) which allows any District Court to summon parties  
7 from another district if the “ends of justice require” it.  
8

9 40. This Court has personal jurisdiction over Bot Sentinel because it directed conduct at  
10 this forum when it participated in the Enterprise. Exercise of jurisdiction over Bot  
11 Sentinel is reasonable because it conspired with Defendants to destroy Goodman’s  
12 business and reputation and terminate his access to social media using Bot Sentinel  
13 technology under Bouzy’s control with the objective of harming Goodman. This  
14 Court also has personal jurisdiction over Bot Sentinel because it participated in a  
15 scheme in violation of 18 U.S. Code § 1513(b)(2) to retaliate against Goodman for  
16 bringing legal action against it and Bouzy. This Court also has personal jurisdiction  
17 over Bot Sentinel under 18 U.S.C. § 1965(b) which allows any District Court to  
18 summon parties from another district if the “ends of justice require” it.  
19  
20

21 41. This Court has personal jurisdiction over Sweigert because he directed conduct at this  
22 forum when he participated in the Enterprise. The exercise of jurisdiction over  
23 Sweigert is reasonable because he conspired with Defendants to destroy Goodman’s  
24 business and reputation and terminate his access to social media by conspiring with  
25 Bouzy to use Bot Sentinel technology under Bouzy’s control with the objective of  
26  
27

1        harming Goodman. This Court also has personal jurisdiction over Sweigert because  
2        he participated in a scheme in violation of 18 U.S. Code § 1513(b)(1) and (2) to  
3        retaliate against Goodman for filing an Amicus Curiae brief in support of Cable News  
4        Network (“CNN”) and other things. This Court also has personal jurisdiction over  
5        Sweigert under 18 U.S.C. § 1965(b) which allows any District Court to summon  
6        parties from another district if the “ends of justice require” it.  
7

8        42. This Court has personal jurisdiction over Webb because he directed conduct at this  
9        forum when he participated in the Enterprise. The exercise of jurisdiction over Webb  
10       is reasonable because he conspired with Defendants to destroy Goodman’s business  
11       and reputation and terminate his access to social media with the objective of harming  
12       Goodman. This Court also has personal jurisdiction over Webb because he  
13       participated in a scheme in violation of 18 U.S. Code § 1513(b)(1) and (2) to retaliate  
14       against Goodman for filing an Amicus Curiae brief in support of CNN and other  
15       things, by filing a frivolous retaliatory lawsuit against Goodman. This Court also has  
16       personal jurisdiction over Webb under 18 U.S.C. § 1965(b) which allows any District  
17       Court to summon parties from another district if the “ends of justice require” it.  
18

19       43. This Court has personal jurisdiction over Wittes because he directed conduct at this  
20       forum when he participated in the Enterprise. The exercise of jurisdiction over Wittes  
21       is reasonable because Wittes conspired with Defendants to destroy Goodman’s  
22       business and reputation and terminate his access to social media by directing Bouzy  
23       to use Bot Sentinel technology under Bouzy’s control with the objective of harming  
24       Goodman. This Court also has personal jurisdiction over Wittes because he  
25  
26  
27

1 participated in a scheme in violation of 18 U.S. Code § 1513 to retaliate against  
2 Goodman for bringing legal action against Bouzy and Bot Sentinel by paying Bot  
3 Sentinel so it could retain Ballard Spahr for its legal defense. This Court has personal  
4 jurisdiction over Wittes under 18 U.S.C. § 1965(b) which allows any District Court to  
5 summon parties from another district if the “ends of justice require” it.  
6

7 44. This Court has personal jurisdiction over Jankowicz because she directed conduct at  
8 this forum when she participated in the Enterprise. The exercise of jurisdiction over  
9 Jankowicz is reasonable because she conspired with Defendants to destroy Plaintiff’s  
10 business and reputation and terminate his access to social media by making false  
11 claims in violation of 22 U.S. Code § 612 and false statements to law enforcement in  
12 Arlington, VA with the objective of harming Goodman. This Court has personal  
13 jurisdiction over Jankowicz under 18 U.S.C. § 1965(b) which allows any District  
14 Court to summon parties from another district if the “ends of justice require” it.  
15

16 45. This Court has personal jurisdiction over Sharp because he directed conduct at this  
17 forum when he participated in the Enterprise. The exercise of jurisdiction over Sharp  
18 is reasonable because he conspired with Defendants to destroy Goodman’s business  
19 and reputation and terminate his access to social media by wrongfully bringing action  
20 against Goodman’s dormant corporation MSD, with the objective of deliberately  
21 harming Goodman. This Court also has personal jurisdiction over Sharp because he  
22 wrongfully caused tax-exempt funds to be used in violation of New York Not-For-  
23 Profit Corporation Law - NPC § 712-a and failed to disclose his interest in a private,  
24 for-profit business while employed as CEO of a tax-exempt corporation. This Court  
25  
26  
27

1 also has personal jurisdiction over Sharp because he participated in a scheme to  
2 commit fraud on the Court in violation of 18 U.S. Code § 1343 by falsely claiming  
3 his private, for-profit corporation Sharp Things, LLC was inactive. This Court has  
4 personal jurisdiction over Sharp under 18 U.S.C. § 1965(b) which allows any District  
5 Court to summon parties from another district if the “ends of justice require” it.  
6

7 46. This Court has personal jurisdiction over Esquenet because she directed conduct at  
8 this forum when she participated in the Enterprise. The exercise of jurisdiction over  
9 Esquenet is reasonable because she conspired with Defendants to destroy Goodman's  
10 business and reputation and terminate his access to social media by participating in a  
11 scheme to wrongfully bring action against MSD, with the objective of deliberately  
12 harming Goodman. This Court also has personal jurisdiction over Esquenet because  
13 she wrongfully accepted tax-exempt funds used in violation of New York Not-For-  
14 Profit Corporation Law - NPC § 712-a. This Court also has personal jurisdiction over  
15 Esquenet because she participated in a scheme to commit fraud on the Court in  
16 violation of 18 U.S. Code § 1343 and New York Judiciary Law - JUD § 487 with the  
17 express intent of harming Goodman by falsely claiming Sharp’s private, for-profit  
18 corporation Sharp Things was inactive. This Court has personal jurisdiction over  
19 Esquenet under 18 U.S.C. § 1965(b) which allows any District Court to summon  
20 parties from another district if the "ends of justice require" it.  
21  
22  
23

24 47. This Court has personal jurisdiction over ATAS because it directed conduct at this  
25 forum when it participated in the Enterprise. The exercise of jurisdiction over ATAS  
26 is reasonable because it conspired with Defendants to financially damage Goodman  
27



1 by wrongfully bringing action against Goodman's dormant New York corporation  
2 MSD, with the objective of harming Goodman. This Court also has personal  
3 jurisdiction over ATAS because it violated its own by-laws and authorized tax-  
4 exempt purpose by wrongfully causing tax-exempt funds to be used in violation of  
5 New York Not-For-Profit Corporation Law - NPC § 712-a. This Court also has  
6 personal jurisdiction over ATAS under 18 U.S.C. § 1965(b) which allows any District  
7 Court to summon parties from another district if the "ends of justice require" it.  
8

9 48. This Court has personal jurisdiction over Berlin because he directed conduct at this  
10 forum when he participated in the Enterprise. The exercise of jurisdiction over Berlin  
11 is reasonable because he conspired with Defendants to intimidate Goodman with  
12 harassing extrajudicial letters after he was alerted by a Tweet sent by Sweigert and  
13 prior to appearing as counsel for Defendants Bouzy and Bot Sentinel in violation of  
14 18 U.S. Code § 1503.  
15

16 49. This Court has personal jurisdiction over Mishkin because he directed conduct at this  
17 forum when he participated in the Enterprise. The exercise of jurisdiction over  
18 Mishkin is reasonable because he conspired with Defendants to intimidate Goodman  
19 with harassing extrajudicial letters after he was alerted by a Tweet sent by Sweigert  
20 and prior to appearing as counsel for Defendants Bouzy and Bot Sentinel in violation  
21 of 18 U.S. Code § 1503.  
22

23 50. This Court has personal jurisdiction over Loury because he directed conduct at this  
24 forum when he participated in the Enterprise. The exercise of jurisdiction over Loury  
25 is reasonable because he conspired with Defendants to file a forged and fraudulent  
26  
27

1 brief in the Eastern District of Michigan in furtherance of a scheme to defraud  
2 Goodman and in violation of 18 U.S.C. §§ 1343, 1503, 1513. This Court also has  
3 personal jurisdiction over Loury under 18 U.S.C. § 1965(b) which allows any District  
4 Court to summon parties from another district if the “ends of justice require” it.  
5

### 6 **FACTUAL BACKGROUND**

7 18 U.S.C. § 1962 makes it unlawful for any person to receive any income derived,  
8 directly or indirectly, from a pattern of racketeering activity. Section 1962(b) prohibits a person  
9 from using a pattern of racketeering activity to acquire or maintain control over an enterprise.  
10 Section 1962(c) prohibits a person from conducting the affairs of an enterprise through a pattern  
11 of racketeering. When Congress enacted the RICO statute in 1970, it included a civil remedy  
12 that allows private parties to sue for injuries to “business or property” caused “by reason of” a  
13 defendant’s violation of RICO. The civil remedy provision requires a plaintiff to prove:  
14

- 15 (1) a violation of a § 1962 prohibited act;
- 16 (2) injury to business or property; and
- 17 (3) that the defendant’s violation caused the injury.

18 Defendants in this case have engaged with Sweigert’s Cyber Militia in order to conduct a  
19 wide-ranging pattern of racketeering activity that began in 2017 and began causing direct and  
20 proximate financial damage to Goodman and his business and property in 2020, continuously up  
21 to and including today. Defendants attempt, in an ongoing fashion, to conceal their efforts using  
22 sophisticated technology including encrypted and clandestine messaging techniques like the  
23 Twitter Virtual Private Network (“TVPV”) identified by Goodman and artificial intelligence  
24 tools including Bot Sentinel software. Defendants continuously abuse regularly issued legal  
25  
26  
27

process and employ deceptive legal tactics designed to manipulate and obstruct both civil and criminal justice while separately serving to hide their individual culpability and direct or indirect coordination between them. This activity is commonly known as lawfare, the weaponization of legal process. Despite strenuous efforts to conceal their pattern of racketeering, evidence presented herein will prove defendants illegally formed and actively participated in the Enterprise with common objectives including the destruction of Goodman’s business and public reputation, extortion of money from him via vexatious and fraudulent litigation, and the total elimination of his access to social media based on the false pretext of spreading disinformation. The Enterprise operates both online and in physical “meat space” as a dynamic collective which Sweigert himself refers to as a (“Cyber Militia”). The Cyber Militia enables coordinated activity through deceptive anonymous online accounts and a multitude of clandestine, encrypted communication schemes intended to amplify Cyber Militia members’ efforts and create the false perception of authentic outcomes that disfavor Goodman, damage his reputation as an investigative journalist, and aim to destroy him financially.

### CIVIL RICO CLAIMS

“Racketeering activity” is defined to include a variety of state and federal predicate crimes *See* 18 U.S. Code § 1961. RICO is not violated by a single act or even a short-term series of occurrences. Civil RICO plaintiffs must describe with specificity a “pattern” of racketeering activity that consists of long-term, ongoing, organized conduct. Persons convicted of violating RICO’s criminal provisions are subject to imprisonment, but a civil RICO action cannot directly result in a conviction. Civil litigants cannot prosecute individuals for violations of criminal

1 statutes. However, the civil remedy within the RICO statute provides a private cause of action to  
2 sue in federal court to recover treble damages caused by a violation.

3 Elements of a RICO violation are;

- 4 (a) a culpable “person” who,  
5 (b) willfully or knowingly,  
6 (c) commits or conspires to the commission of “racketeering activity”,  
7 (d) through a “pattern”,  
8 (e) involving a separate “enterprise” or “association in fact,” and,  
9 (f) an effect on interstate or foreign commerce.  
10  
11

12 In this case, each of the defendants are individually a “culpable person” even those who  
13 initially encountered the Enterprise unwittingly. Even after being informed of the existence of  
14 the Enterprise, defendants voluntarily chose to convert themselves into a “culpable person” by  
15 willfully joining and participating in the pattern of racketeering activity.  
16

17 Because RICO is predicated on criminal conduct, plaintiffs are required to establish that  
18 each defendant intended to engage in racketeering conduct with actual knowledge of the illegal  
19 activities. Defendants in this case have not plead ignorance to their actions or negligence in the  
20 conduct Goodman describes. They each willfully engaged in the pattern of racketeering activity  
21 described. *See, e.g., Doug Grant, Inc. v. Greate Bay Casino Corp.*, 232 F.3d 173, 185-87 (3d Cir.  
22 2000) (affirming dismissal of suit by casino card counters who complained about casino  
23 countermeasures like frequent deck shuffling because such actions did not qualify as RICO  
24 predicate acts). Defendants in this case were not engaged in normal activities associated with  
25  
26  
27

1 legitimate conduct but rather willfully targeted Goodman, his business, and his property with  
2 their pattern of fraudulent, and malicious conduct.

3 **I. Multimedia System Design, Jason Goodman, and Crowdsource the Truth**

4 Goodman is the sole proprietor of MSD, a corporation he founded in 1994 originally  
5 focused on computer network design and maintenance for graphic arts and multimedia  
6 professionals. In May of 1998, Goodman applied for and received the assumed name  
7 “Multimedia Software Design” to better reflect the evolving nature of the business. Years later,  
8 the company shifted focus to 3D and stereoscopic video production. Goodman again applied for  
9 an assumed name with the New York Department of State and established “21st Century 3D”.  
10

11 **(EXHIBIT C)**

12 Goodman had a lucrative career in Hollywood for many years where he was recognized  
13 as one of the world’s foremost experts in stereoscopic cinematography and 3D camera design  
14 and development. Multimedia System Design, INC., D.B.A. 21st Century 3D operated offices in  
15 New York and Los Angeles. In or around 2013, 3D moviegoing and production crashed and  
16 virtually all of Hollywood’s 3D providers including 21st Century 3D ceased operation.  
17

18 Goodman returned to New York in or around 2015 and worked to re-establish himself in a  
19 market that no longer demanded stereoscopic cinematographers. MSD remained active and in  
20 good standing but Goodman’s role as CEO focused on rare, occasional, specialized 3D work and  
21 eventually turned to selling the company’s large inventory of valuable professional camera  
22 equipment. At the same time, Goodman engaged in the separate unrelated endeavor of creating  
23 news, information and entertainment videos using inexpensive mobile phones owned by  
24 Goodman, broadcast on a YouTube channel called “Jason Goodman” with shows bearing the  
25  
26  
27

brand name “Crowdsource the Truth” and unrelated to MSD. Leveraging his experience as a producer and cinematographer, and emerging skills as a journalist and talk show host, Goodman built an audience on YouTube and eventually monetized the effort by creating a subscription video service through which individual viewers become monthly sponsors and gain access to sponsor exclusive content on [www.patreon.com](http://www.patreon.com) (“Patreon”), [www.subscribestar.com](http://www.subscribestar.com) (“SubscribeStar”) and [www.odysee.com](http://www.odysee.com) (“Odysee”). MSD is not associated with these platforms or their payment services. Goodman is the sole and exclusive owner of intellectual property and artistic works created by Goodman under the brand name Crowdsource the Truth.

### **FIRST CAUSE OF ACTION**

#### **18 U.S. Code § 1962(b)**

51. Plaintiff incorporates by reference each and every allegation set forth in the preceding paragraphs as if fully stated herein.

52. 18 U.S. Code § 1962(b) makes it unlawful for any person through a pattern of racketeering activity to acquire or maintain, directly or indirectly, any interest in or control of any enterprise which is engaged in, or the activities of which affect, interstate or foreign commerce.

53. Sweigert illegally obtained interest and exercises control over the Enterprise he describes as a militia or some other component of the United States National Guard without any legal authority to do so in violation of 18 U.S. code § 1962(b).

54. Sweigert’s Cyber Militia is an enterprise engaged in and whose activities affect interstate commerce. Inter alia, Sweigert currently markets and sells a book entitled “Report: The Port of Charleston Dirty Bomb Hoax and Social Media Liability” which

contains false, unfounded, and defamatory statements alleging Goodman engaged in domestic terrorism, hacking and other crimes. These known false statements are solely intended to harm Goodman and violate 18 U.S. code §§ 1343 and 1513.

55. Defendants agreed to and did conduct and participate in the conduct of the Enterprise's affairs through a pattern of racketeering activity and for the unlawful purpose of intentionally defrauding Plaintiff. Specifically:

- a. Sweigert and Webb committed wire fraud in violation of 18 U.S. code § 1343 in the course of deceiving Goodman during a YouTube broadcast on June 14, 2017 and then publishing a book blaming Goodman for the closure of the Port of Charleston and to form the basis for a series of vexatious legal actions.
- b. Sweigert, Sharp, Esquenet and ATAS committed wire fraud in violation of 18 U.S. code § 1343 on July 28, 2020, when they caused a fraudulent email falsely alleging Goodman violated ATAS' copyright to prompt a legal dispute between ATAS and Goodman.
- c. Sweigert, Sharp, Esquenet and ATAS committed wire fraud in violation of 18 U.S. code § 1343 on August 20, 2020, when calculated a scheme intended to delay a false copyright complaint with YouTube so it would strategically obstruct Goodman and prevent him from broadcasting during the 2020 Presidential election.
- d. Even if the Court determines that statements made to social media providers by defendants about copyright infringements or content that violates the relevant Terms of Service are protected under New York State's doctrine of

litigation privilege, delaying such statements to execute a calculated scheme intended to harm Goodman or deprive him of rights or property is not a component of litigation privilege. This calculated delay makes the fraudulent complaint a predicate act under RICO and a violation of 18 U.S. code § 1343 and provides strong evidence of the coordination alleged by Goodman.

- e. Sweigert, Webb and Loury violated 18 U.S. Code § 1343, 18 U.S. Code § 1503, and § 1513 on June 21, 2021, when they forged a filing and caused it to be placed on the ECF in the Eastern District of Michigan with the express intent of harming Goodman. **(EXHIBIT D)**
- f. Bouzy violated 18 U.S. Code § 1343 and 18 U.S. Code § 1513 on March 18, 2022, when he made a false statement to Twitter with the express intent of harming Goodman and in retaliation for being sued.
- g. Wittes and Bouzy violated 18 U.S. Code § 1951 on December 19, 2021 when Wittes incited Bouzy to cyber harass Goodman to extort Goodman into terminating broadcasts of factual information that is unfavorable to Wittes.
- h. Bouzy, Mishkin and Berlin violated 18 U.S. Code § § 1343, 1503 and 1513 when they sent harassing emails to Goodman prior to Mishkin and Berlin legally representing Bouzy with the intent of harming Goodman.
- i. Sweigert and Jankowicz violated 18 U.S. Code § § 1343, 1503, and 1513 on January 4, 2023, when they made a false statement to Twitter with the express intent to harm Goodman and in retaliation for being sued.



1 j. Sweigert, Jankowicz and Wittes violated 18 U.S. Code § § 1343, 1503, and  
2 1513 on January 6, 2023, when they made false statements to law enforcement  
3 in Arlington, VA with the express intent of harming Goodman by falsely  
4 claiming Goodman threatened Jankowicz to wrongfully obtain an order of  
5 protection against Goodman.  
6

7 56. In order to establish standing under 1962(b) the Second Circuit has determined  
8 plaintiffs' "damages must be different from the damages that flow from the predicate  
9 acts themselves." *Vashovsky v. Zablocki*, 2022 NY Slip Op 31497(U), ¶ 3 (Sup. Ct.)  
10

11 57. In this case, individual predicate acts did pin prick damage, but only the cumulative  
12 effect of the collective actions of the Enterprise, and the pattern of racketeering  
13 activity it engaged in, has resulted in proximate pecuniary damage from the loss of  
14 access to business property including social media accounts, unfair advantage gained  
15 in multiple civil actions resulting in financial damage and loss of business revenue.  
16

17 58. Defendants became associated with the Enterprise at various times between 2017 and  
18 2023 and through varied circumstances. They coordinate their efforts in executing  
19 their common goal of extorting money from Goodman through vexatious lawsuits  
20 and by denying Goodman access to social media through mass complaint campaigns  
21 intended to forcibly extort Goodman into terminating broadcasts of information that  
22 is unfavorable to defendants.  
23

24 59. Through a coordinated effort and with the cooperation of all Count I defendants,  
25 Sweigert has engaged in a pattern of racketeering activity including the formation of a  
26 Cyber Militia Enterprise and a years long, ongoing lawfare campaign against  
27

1 Goodman intended to destroy his business, deprive him of property and money and  
2 end his ability to broadcast the findings of his investigative journalism by terminating  
3 his access to social media.  
4

5 **SECOND CAUSE OF ACTION**

6 **18 U.S. Code § 1962(c)**

7 60. Plaintiff incorporates by reference each and every allegation set forth in the preceding  
8 paragraphs as if fully stated herein.

9 61. In order to establish standing for a civil RICO claim under 1962(c): (1) the  
10 plaintiff must be a “person” (2) who sustains injury (3) to its “business or property” (4)  
11 “by reason of” the defendant’s violation of § 1962.  
12

13 62. The Supreme Court has rejected the Second Circuit finding that required a RICO  
14 plaintiff to demonstrate a “racketeering injury” distinct from the harm caused by the  
15 RICO predicate acts.  
16

17 63. Goodman is the person who has sustained injury to his business and property by  
18 reason of the Enterprise’s ongoing racketeering activity.

19 64. Acting as individuals, Sharp, Esquenet and ATAS could not have known  
20 Goodman owned MSD because it is not directly associated with Crowdsourcethe Truth  
21 or defendants’ allegations of copyright infringement, trademark dilution or other claims.  
22

23 65. The false entity MSDI was a product of the Enterprise, and defendants learned of  
24 it through their participation in the Enterprise.

25 66. Defendants’ used knowledge of the false entity MSDI to harm Goodman by suing  
26 the false entity with the deliberate intent of denying Goodman the right to a fair trial.  
27

1       67. Defendant Loury participated, directly or indirectly, in the conduct of the  
2       Enterprise's affairs through a pattern of racketeering activity when he conspired with  
3       Sweigert and Webb to file a fraudulent document in the Eastern District of Michigan.

4       68. Defendant Bouzy participated, directly or indirectly, in the conduct of the  
5       Enterprise's affairs through a pattern of racketeering activity when he used information  
6       provided by Sweigert to cyberstalk, harass, and defame Goodman.

7       69. Defendants Mishkin and Berlin participated, directly or indirectly, in the conduct  
8       of the Enterprise's affairs through a pattern of racketeering activity when they harassed  
9       Goodman with emails and letters while they did not legally represent defendants.

10       70. Defendant Jankowicz participated, directly in the conduct of the Enterprise's affairs  
11       through a pattern of racketeering activity when she collaborated with Sweigert to  
12       transmit a fraudulent claim to Twitter in violation of 18 U.S. Code § 1343 alleging  
13       Goodman violated Twitter policy with the express intent of harming Goodman.

14       71. Defendant Jankowicz participated, directly in the conduct of the Enterprise's affairs  
15       through a pattern of racketeering activity when she collaborated with Sweigert to  
16       transmit a fraudulent claim to the Arlington, VA Police when she made a false  
17       statement alleging Goodman had threatened her with violence to obtain a fraudulent  
18       order of protection against Goodman.

19                                   **THIRD CAUSE OF ACTION**

20                                   **18 U.S. Code § 1962(d)**

21       72. Plaintiff incorporates by reference each and every allegation set forth in the preceding  
22       paragraphs as if fully stated herein.

1       73. As set forth above, defendants agreed and conspired to violate 18 U.S.C. §  
2       1962(b) and (c). Specifically;

3       74. Defendants Sharp, Esquenet and ATAS agreed and conspired to concoct a false  
4       email to create a pretext for suing Goodman. They further agreed to delay a complaint  
5       based on the false email for nearly one month so their complaint would cause maximum  
6       harm to Goodman, demonstrating that harming Goodman was their primary interest, not  
7       curing the alleged injury. They then agreed to sue a false corporation imagined by the  
8       Enterprise and named to closely resemble a corporation owned by Goodman to prevent  
9       Goodman from defending himself pro se and to gain an unfair advantage in litigation.  
10      They agreed to harass counsel hired by Goodman and compel a withdrawal followed by  
11      default judgement to gain an advantage in the litigation. Despite being offered a  
12      settlement that would cure their injury, they decided to conduct and participate in the  
13      conduct of the affairs of the enterprise through the pattern of racketeering activity  
14      described.

15      75. Defendants Sweigert, Webb and Louri agreed and conspired to forge a document  
16      and file it in the Eastern District of Michigan in an effort to draw Goodman into  
17      litigation. They did this with the intent to harm Goodman and in violation of 18 U.S.  
18      code §§ 1343, 1502 and 1513.

19      76. Defendants Sweigert, Wittes and Bouzy agreed and conspired to make false  
20      claims to Twitter with the express intent of harming Goodman.

21      77. Defendants Bouzy, Mishkin and Berlin agreed and conspired to harass Goodman  
22      with extrajudicial communications in an effort to gain an advantage in litigation.



1 83. Defendants Webb, Sweigert and Bouzy defamed Goodman when they knowingly  
2 published false and defamatory statements in general that accused Goodman of rape  
3 when they knew such statements to be false and inherently damaging per se libel.  
4

5 84. The Defendants made these statements to third parties knowing they were false  
6 and without privilege, while deliberately ignoring the true facts of the matter.

7 85. Defendants made these statements with actual malice, and with intent to expose  
8 Goodman to public hatred and loss of professional and personal reputation with the  
9 express intent of damaging Goodman in his business and profession.  
10

11 86. Defendant Bouzy defamed Goodman when he knowingly published false  
12 conclusory statements to third parties on Twitter declaring Goodman had falsely accused  
13 Wittes of deliberately misleading the public with regard to the death of Peter W. Smith.

14 87. Defendant Bouzy made these defamatory statements with the full knowledge that  
15 Goodman is a professional investigative journalist and his reputation for truthfulness is  
16 inherently valuable in his profession.  
17

18 88. Defendant Bouzy made these statements even though he himself agreed in a  
19 phone call that the death was suspicious, and the police investigation was superficial.

20 89. Defendant Bouzy made these statements with actual malice and the express intent  
21 of damaging Goodman in his professional reputation and causing proximate pecuniary  
22 damages to Goodman.  
23

24 90. At the time the Defendants made the statements, they knew the statements to be  
25 false and defamatory or alternately, chose to deliberately ignore the truth.  
26  
27

1 91. Defendants made these false and defamatory statements with actual malice, and  
2 the express intent to malign and injure the Plaintiff.

3 92. Defendant Bouzy has hundreds of thousands of Twitter followers, dozens of  
4 which read, and acknowledged or responded to Defendants' false and defamatory  
5 statements clearly indicating they had been published to third parties without privilege or  
6 authorization.  
7

8 93. Even if the Court finds Goodman's statements are an admission to a rape  
9 accusation, Goodman was unequivocal in his repeated statements that the accusation was  
10 false, unsubstantiated, and originated from a person who did not even claim to be the  
11 alleged victim, know the alleged victim or have spoken to the alleged victim.  
12

13 94. Bouzy repeated the statement with reckless negligence and made no effort to confirm  
14 the underlying facts of the allegation. Because the crime of rape is so heinous, any  
15 allegation of any such involvement is inherently damaging to an individual's  
16 reputation. Bouzy's willful repetition of a known false accusation is at least  
17 defamation by implication. In *Golan v Daily News*, the Second Circuit Court  
18 established a standard for determining defamation by implication, stating in relevant  
19 part, "The court has found that where there is a claim for defamation by implication  
20 and the factual statements are found to be substantially true, the plaintiff must make a  
21 rigorous showing that the language of the communications as a whole can be  
22 reasonably read both to impart a defamatory inference and to affirmatively suggest  
23 that the author intended or endorsed that inference. *Golan v. Daily News, L.P.*, 2022  
24 NY Slip Op 22314, ¶ 1, 77 Misc. 3d 258, 260, 175 N.Y.S.3d 871, 876 (Sup. Ct.). A  
25  
26  
27

1 reasonable observer reading Bouzy's statements would be likely to conclude  
2 Goodman had been involved in rape, resulting in the existence of an accusation, and  
3 that Bouzy was endorsing the inference by gleefully repeating it all over Twitter.  
4 Bouzy was not engaged in any journalistic effort when he published the tweet. Bouzy  
5 was not engaged in anti-rape activism or some other meaningful activity. Bouzy  
6 should have made a good faith effort to substantiate the truthfulness of the underlying  
7 claims before publishing his tweet or repeating the claims with no fundamental  
8 purpose other than the actual malice of deliberately damaging Goodman with a  
9 known false statement or endorsing the implication of a known false statement.  
10  
11

## 12 **FIFTH CAUSE OF ACTION**

### 13 **Abuse of Process**

14 95. Plaintiff incorporates by reference each and every allegation set forth in the  
15 preceding paragraphs as if fully stated herein.

16 96. Defendant Sweigert abused regularly issued civil process with the intent to harm  
17 Goodman without a legitimate excuse or justification, and perverted use of the process to  
18 achieve the collateral objective of destroying Goodman's business and overwhelming  
19 him with vexatious litigation when he brought multiple civil actions and attempted to  
20 intervene in existing civil actions against Goodman across a wide range of U.S. District  
21 Courts including South Carolina, the Southern District of New York, the Eastern District  
22 of Michigan and the Eastern District of Virginia.

23 97. Defendant Sharp abused regularly issued civil process with intent to harm  
24 Goodman when he endeavored to create a fraudulent excuse in his wrongful attempt to  
25  
26  
27



1 justify vexatious litigation against a company owned by Goodman for a parody image  
2 posted on the internet by Goodman in violation of 47 U.S. Code § 230. Sharp perverted  
3 the use of the process and applied the power of the Court in a manner not intended by the  
4 law to achieve the collateral objective of destroying Goodman's popular subscription  
5 video service for the improper purpose of preventing Goodman from broadcasting during  
6 the 2020 election. Sharp did this with malicious intent and for the improper purpose of  
7 his own political and financial benefit and that of his preferred Presidential candidate.  
8

9 98. Defendants violated 18 U.S. Code § 1512(c)(2) when Sweigert harassed Snyder,  
10 the attorney retained to represent Goodman's corporation. Defendants abused regularly  
11 issued civil process with intent to harm Goodman for the express purpose of denying him  
12 the right to a fair trial and the right to defend himself pro se causing proximate harm to  
13 Goodman in the form of significant financial damages, damages to his business and  
14 reputation, and loss of property in the form of his valuable branded social media accounts  
15 that his business relied upon.  
16

## 17 **SIXTH Cause of Action**

### 18 **Civil Conspiracy**

19 99. Plaintiff incorporates by reference each and every allegation set forth in the  
20 preceding paragraphs as if fully stated herein.  
21

22 100. Defendants Sweigert, Sharp, ATAS, and Esquenet entered into a civil conspiracy  
23 when they agreed to create a pretext under which they intended to sue a corporation  
24 owned by Goodman for an internet post made by Goodman in his personal capacity in  
25  
26  
27

1 violation of 47 U.S. Code § 230 and with the express intent of harming Goodman and  
2 extorting him into ceasing news broadcasts during the 2020 Presidential election.

3 101. In furtherance of the civil conspiracy, Sweigert caused an email to be sent from an  
4 allegedly anonymous email address in violation of 18 U.S. Code § 1343 with the express  
5 intent of creating a pretext for a lawsuit against a corporation owned by Goodman that  
6 Sharp, ATAS, and Esquenet had no knowledge of prior to entering the conspiracy with  
7 Sweigert. The conspiracy caused acute proximate pecuniary damage to Goodman by  
8 forcing him to retain an attorney who failed to defend Goodman's corporation according  
9 to Goodman's instructions and then withdrew as a direct result of harassment by the  
10 Enterprise. Defendants calculated their actions specifically to harm Goodman or  
11 otherwise should have known his injuries were a foreseeable result of their conspiracy.

12 102. Defendants Webb and Sweigert entered into a civil conspiracy with non-party  
13 Loury in violation of 18 U.S. Code §§ 1343 and 1513 when they caused a fraudulent  
14 document to be filed with the Court in the Eastern District of Michigan.

15 103. Defendants did this with the express intent of harming Goodman by denying him  
16 his rights to a fair trial and with the express intent of damaging Goodman with costs and  
17 fees associated with defending malicious, vexatious litigation.

18 104. Defendants committed this overt act, knowing the case would otherwise be  
19 dismissed if not for the conspiracy to file the fraudulent document. Defendants  
20 proceeded with the full knowledge that their actions would proximately damage  
21 Goodman and they did so with malicious intent.

1 105. Defendants knew or otherwise should have known the actions of their conspiracy  
2 would harm Goodman in the form of pecuniary damages due to burdensome litigation.

3 106. Defendants Sweigert and Webb enlisted each of the other defendants to cooperate  
4 with them for a common purpose and towards a common goal of damaging Goodman and  
5 wrongfully denying him access to his property.  
6

7 107. The Defendants' racketeering activity affected interstate commerce by  
8 proximately damaging Goodman in the state of New York while utilizing coconspirators  
9 in New Jersey, Connecticut, Washington D.C. and other states and also through the  
10 transmission of false statements over the wires of the internet and or phones to service  
11 providers and social media platforms in California, Wyoming and New Hampshire.  
12

13 108. Defendants Webb, Sweigert, Bouzy, Wittes and Jankowicz at a minimum, derived  
14 income as a direct or indirect result of their participation in the Enterprise.

15 109. As A direct and proximate result of the defendants' conspiracy, the overt acts  
16 taken in furtherance of that conspiracy, and violations of 18 U.S.C. § 1962(d), Goodman  
17 has been injured in his business and property in that;  
18

19 a. Goodman's annual income has been reduced by nearly 50% since 2020 when  
20 pecuniary damage began.

21 b. Goodman has completely lost access to his most valuable social media  
22 properties, including a YouTube channel titled "Jason Goodman" with over  
23 119,000 regular subscribers which was the target of a scheme calculated and  
24 executed by the Enterprise to strategically delay a false copyright complaint  
25  
26  
27

1 by nearly a month to specifically prevent Goodman from broadcasting during  
2 the 2020 Presidential election.

3 c. Goodman also lost access to a valuable Twitter account (“@csthetruth”) with  
4 over 26,000 followers due to false statements by Sweigert, Bouzy, and  
5 Jankowicz  
6

7 d. Goodman has lost access to his first amendment rights for the next two years  
8 with regard to any factual reporting or any commentary whatsoever regarding  
9 defendant Jankowicz due to a scheme calculated by the Enterprise intended to  
10 obtain a fraudulent order of protection against Goodman.  
11

12 e. Goodman has lost access to his second amendment rights for the next two  
13 years due to a scheme calculated by the Enterprise intended to obtain a  
14 fraudulent order of protection against Goodman.  
15

16 f. Goodman has lost access to valuable branded social media accounts that his  
17 business relied upon including Twitter, Facebook and YouTube.

18 110. Plaintiff Goodman suffered reputational damage and substantial pecuniary  
19 damage to his business and his valuable branded social media properties as a proximate  
20 result of the Defendants’ racketeering activity.

21 **PRAYER FOR RELIEF**

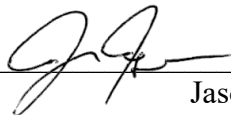
22 WHEREFORE, Plaintiff prays the Court will enter judgement in his favor and issue an  
23 order for the following relief:  
24

- 25 1. Declaring that the Defendants statements were libelous and defamatory.  
26 2. Declaring Defendants vexatious litigants and mandating that each first seek leave  
27

- 1 of this Court before bringing future litigation against Goodman or any company  
2 owned or utilized by Goodman effective immediately and on into perpetuity.  
3
- 4 3. Granting an order compelling Defendants ATAS, Sharp and Esquenet to issue a  
5 public apology to be approved by Goodman prior to publication admitting to their  
6 wrongdoing and absolving Goodman and MSD of false claims. The release is to be  
7 issued in the Hollywood Reporter, Variety, and Bloomberg Law and must occupy  
8 at least as much editorial space as the September 4, 2020 article entitled  
9 “Television Academy Sues After Emmy Statuette Given Coronavirus”  
10
- 11 4. Finding all Defendants jointly and severally liable to the extent of,  
12 a. treble the damages incurred due to Defendants’ unlawful activity including  
13 attorneys’ fees and costs associated with defending Goodman’s dormant  
14 corporation pursuant to Federal RICO statutes,  
15 b. costs and expenses spent bringing and defending this and other lawsuits  
16 caused by Defendants and,  
17 c. \$2,200,000 in lost business revenue and,  
18 d. \$20,000,000 or an amount otherwise to be decided by a jury in the form of  
19 punitive damages for Defendants’ illegal, fraudulent and defamatory actions.  
20
- 21 5. Granting Goodman relief for money damages for all economic losses  
22 including, but not limited to, lost past and future earnings; and for  
23 compensatory damages; and for punitive damages; and for interest at the  
24 maximum legal rate on all sums awarded; and for such other and such further  
25 relief as the Court deems just and proper.  
26  
27

Signed this 28<sup>th</sup> day of February 2023

Respectfully submitted,



Jason Goodman, Plaintiff, Pro Se  
252 7<sup>th</sup> Avenue Apt 6s  
New York, NY 10001  
(323) 744-7594  
[truth@crowdsourcethetruth.org](mailto:truth@crowdsourcethetruth.org)

**(EXHIBIT A)**

## **Expanding the role of National Guard Cyber Units to support disaster response and recovery and make a Cyber Militia a reality**

**January 2014**

**Author: Dave Sweigert, M.Sci., CISSP, CISA, PMP**

### **ABSTRACT**

**Private organizations would be well advised to be aware of the involvement of National Guard cyber warfare units in responding to attacks on critical infrastructure. Increased interaction with Guard units may be appropriate for entities concerned with community-wide cyber resiliency.**

### ***Background***

This year the passage of the National Defense Authorization Act (NDAA) by the U.S. Congress (used to supply the Pentagon with another year's budget) came with cybersecurity strings attached – the requirement for a comprehensive domestic cyber warfare assessment of how the National Guard would support defensive cyber warfare operations and support missions of the U.S. Department of Homeland Security.

In sum, there is likely to be a new cybersecurity player in the Critical Infrastructure – Key Resources (CIKR) arena, the National Guard.

### ***Is this the creation of a Cyber Militia?***

**Cyber Militias:** these are non-state sponsored collections of volunteers that can act in a militant offensive and defensive manner in cyber space. These groups can be loosely organized and operate with technical know-how to

accomplish political objectives. The Chinese Eagle Union Hacker Group is one example of a “Cyber Militia”.

Attacks launched by such groups that breach network cybersecurity are classified as “cyber warfare” by the Pentagon. Doomsday scenarios predict everything from massive failures of the power grid to the destruction of medical data as a consequence of an act of cyber war by such groups, creating “cyber anxiety”.

Many observers have suggested that the language of the 2014 NDAA is a Dr. Strangelovian attempt to “close the cyber militia gap” and keep up with the creation of such militias in Russia, Iran, and North Korea.

**Cyber Warfare:** Both the National Guard Bureau (NGB) and the National Governor's Association (NGA) have openly endorsed the idea of Guard units engaged in civilian defensive cyber warfare operations.



### ***Domestic Cyber Missions***

Until now, the number of Guard units involved in civilian cybersecurity events could be counted with one hand. Examples:

Prior to the 2010 Winter Olympics the network supporting Washington State's Division of Motor Vehicles (DMV) was assessed by a Guard cyber warfare unit. Networks supporting the 2012 Presidential Inauguration were protected by such units and State networks supporting Emergency Management (E.M.) activities have also been accessed by these groups.

Such activities fall within the **National Prevention Framework** "cybersecurity" category as a **PROTECTION** capability.

With the desire of Congress to "close the gap" the scope of such support by Guard units in domestic cyber missions could be expanding. Cascading consequences created by a cyber event are addressed within the **National Response Framework** as a **RESPONSE** and **RECOVERY** activity.

State Governors could certainly activate such units during man-made cyber disasters and to support response and recovery operations in natural disasters, as well as provide support to the U.S. Department of Homeland Security missions. However, only a handful of such states have these elite cyber warfare units.

### ***Integration with the Whole Community Concept***

The Whole Community Approach to Preparedness promoted by Presidential Policy Directive 8 (**PPD-8: National Preparedness**) is a comprehensive and integrated approach to community preparedness for disasters – to include man made cyber events and their cascading consequences.

The increased interaction of public safety agencies and private entities with these National Guard cyber units in support of **PPD-8** should be addressed by the Pentagon. Alignment of Guard cyber capabilities to jointly respond with other Whole Community partners in a realistic approach to a CIKR cyber event (and the associated potential downstream effects on public utilities, medical facilities, transportation arteries, etc.) should be planned for.

Joint planning would help define how these Guard units could more effectively interface with other response agencies during cyber events and disasters. This would give Congress the Cyber Militia capability they are searching.

**About the author:** Dave Sweigert holds certifications as a Certified Information Systems Security Professional, Certified Information Systems Auditor, and Project Management Professional. He has earned Master's degrees in Information Security and Project Management. An Air Force veteran, he is a practitioner of cybersecurity, incident management and CIKR protection. He has consulted to Kaiser Permanente, J2 Global, NASA and the U.S. Army.

**(EXHIBIT B)**

00:00:00:23 - 00:00:02:14

Speaker 1

Hey, everybody, this is Dave. So we're going.

00:00:02:14 - 00:00:03:10

Speaker 2

To get further.

00:00:03:10 - 00:00:04:02

Speaker 1

Into the.

00:00:04:15 - 00:00:05:12

Speaker 2

Cyber warfare.

00:00:05:12 - 00:00:06:16

Speaker 1

Simulation, this war.

00:00:06:16 - 00:00:07:18

Speaker 2

Gaming scenario, if you want to.

00:00:07:18 - 00:00:11:10

Speaker 1

Think of it that way, we're moving fast because.

00:00:11:10 - 00:00:12:17

Speaker 2

I'm working around.

00:00:12:17 - 00:00:30:18

Speaker 1

Waiting for consensus from government people or industry people or people like that. We're moving ahead with the actual scenario that's going to be used by actual infrastructure operators. I guarantee you what we're doing right now is going to be documented and it's.

00:00:30:18 - 00:00:31:15

Speaker 2

Going to be read.

00:00:32:03 - 00:00:34:13

Speaker 1

By several dozen key people.

00:00:34:13 - 00:00:36:00

Speaker 2

That run the critical infrastructure.

00:00:36:00 - 00:00:38:25

Speaker 1

Of the United States. So I'm.

00:00:39:00 - 00:00:40:08

Speaker 2

Encouraging everyone to.

00:00:40:08 - 00:01:01:00

Speaker 1

Participate because we are actually forming national policy indirectly. We're inputting in the national policy what we think is happening. And I think this is really important. I have a passion for this. That's why I'm sticking with it. You guys have been doing great. You've been keeping up, you've been researching things. I think I'm.

00:01:01:13 - 00:01:02:21

Speaker 2

Extremely proud.

00:01:03:00 - 00:01:09:04

Speaker 1

Of the way you guys have showing interest in this. So you should be congratulated for your interest in this subject matter.

00:01:09:04 - 00:01:10:10

Speaker 2

Thank you very much.

00:01:11:21 - 00:01:14:12

Speaker 1

We're going to look at the beginnings of cyber.

00:01:14:12 - 00:01:15:23

Speaker 2

Warfare for our.

00:01:15:23 - 00:01:19:12

Speaker 1

Discussion. And that's going to begin in Estonia in 2007.

00:01:20:04 - 00:01:21:06

Speaker 2

And our.

00:01:21:20 - 00:01:25:14

Speaker 1

Kick off our beginning date of our discussions is.

00:01:25:14 - 00:01:26:18

Speaker 2

Cyber warfare. It's going to.

00:01:26:18 - 00:01:28:09

Speaker 1

Be the use of cyber.

00:01:28:09 - 00:01:31:24

Speaker 2

Militias. Cyber militias were first.

00:01:31:24 - 00:01:33:09

Speaker 1

Suggested in the Estonia.

00:01:33:09 - 00:01:33:20

Speaker 2

Cyber.

00:01:33:20 - 00:01:46:24

Speaker 1

Attacks when Estonia was losing millions of dollars a day because the websites of their banks, their power company, post office or government agencies.

00:01:46:24 - 00:01:48:14

Speaker 2

Were all under cyber attack.

00:01:48:27 - 00:02:15:13

Speaker 1

They eventually had to cut off all routed traffic coming into the nation. If you read a lot of the international policy documents on this kind of attack, and I'll show you the the title of this document, let me read just a little bit. The Estonian attacks targeted the websites of banks, telecommunications company, media outlets, government agencies. They eventually forced the country to.

00:02:15:13 - 00:02:18:27

Speaker 2

Block all foreign traffic, etc., etc..

00:02:19:11 - 00:02:21:29

Speaker 1

This is when they first began the concept of.

00:02:21:29 - 00:02:25:28

Speaker 2

A cyber militia, a train force of part.

00:02:25:28 - 00:02:33:00

Speaker 1

Time civilians that met a certain standard and that they could be called on in the case of a cyber.

00:02:33:00 - 00:02:33:17

Speaker 2

Attack.

00:02:33:29 - 00:02:34:22

Speaker 1

In peacetime.

00:02:34:22 - 00:02:35:09

Speaker 2

Or war.

00:02:35:09 - 00:02:42:04

Speaker 1

Time to help defend. So the cyber militia concept also came up. Let me I'll.

00:02:42:06 - 00:02:43:23

Speaker 2

Describe it here.

00:02:43:23 - 00:02:48:24

Speaker 1

One possible solution may be that states follow the example of countries that have been subject to.

00:02:48:25 - 00:02:49:21

Speaker 2

Large scale cyber.

00:02:49:21 - 00:02:53:01

Speaker 1

Attacks such as Estonia in 2007 and.

00:02:53:01 - 00:02:53:17

Speaker 2

Support.

00:02:53:17 - 00:02:57:01

Speaker 1

Prop up so-called cyber militias ready to defend the country's critical.

00:02:57:01 - 00:02:57:23

Speaker 2

Infrastructure.

00:02:58:03 - 00:02:59:16

Speaker 1

Against both non-state.

00:02:59:16 - 00:03:00:04

Speaker 2

Actors.

00:03:00:17 - 00:03:18:26

Speaker 1

Cyber criminals and nation states. Members of the cyber militia recruited amongst a pool of civilians with the requisite forensic and I.T. skills would be deployed in both peace and war time in protecting the country's

critical infrastructure. Here, however, only the malicious leadership of this small cadre would be full time staff.

00:03:19:09 - 00:03:19:27

Speaker 2

The rest.

00:03:20:04 - 00:03:21:26

Speaker 1

After completing a cyber bootcamp.

00:03:21:26 - 00:03:23:08

Speaker 2

Would have a predetermined number of.

00:03:23:08 - 00:03:36:23

Speaker 1

Days a can do like being in the National Guard. Yeah, well, the international community has been talking about this concept since 2007. It's all talk, talk, talk. We're actually going to make it happen.

00:03:36:23 - 00:03:39:04

Speaker 2

Here and walk through it.

00:03:39:19 - 00:03:40:21

Speaker 1

And see what we can.

00:03:40:21 - 00:03:41:24

Speaker 2

Learn from the.

00:03:41:24 - 00:03:47:28

Speaker 1

Human dimension and the human dimension. The hysteria dimension is provided by.

00:03:48:07 - 00:03:50:26

Speaker 2

Our friend George Webb, and we're so.

00:03:50:26 - 00:04:02:08

Speaker 1

Embedded into the process we can easily keep an eye on what the what he's doing and use his operations as an example to augment what we're studying. Because most of us know it's just a question of time.

00:04:02:08 - 00:04:04:12

Speaker 2

That George is going to orchestrate something.

00:04:04:12 - 00:04:04:24

Speaker 1

Else like.

00:04:04:24 - 00:04:05:08

Speaker 2

The Port.

00:04:05:21 - 00:04:09:08

Speaker 1

Of Charleston closure, and now he's got his people in.

00:04:09:08 - 00:04:10:10

Speaker 2

England running around.

00:04:10:10 - 00:04:12:12

Speaker 1

England. What are they going to do in England? Are they going.

00:04:12:12 - 00:04:13:02

Speaker 2

To do another.

00:04:13:29 - 00:04:17:13

Speaker 1

Questionable attack? Sorry to use the attack.

00:04:17:13 - 00:04:17:22

Speaker 2

Word.

00:04:17:22 - 00:04:34:15

Speaker 1

But, you know, with all the questions about shutting down the Internet in England right now, you know, that's kind of a very sensitive area, wouldn't you think? So? Of course, this is from the Army War College. They've been talking about these kinds of.

00:04:34:15 - 00:04:35:19

Speaker 2

Operations for a long time.

00:04:35:19 - 00:04:36:01

Speaker 1

Again, it's.

00:04:36:01 - 00:04:37:01

Speaker 2

Lots of talk, talk.

00:04:37:01 - 00:04:47:21

Speaker 1

Talk. I want to point out a white paper. I wrote the link you'll find below. This is called Securing Cyber Infrastructure, utilizing the.



00:04:47:21 - 00:04:49:12

Speaker 2

Culture of Emergency Management.

00:04:50:06 - 00:04:52:15

Speaker 1

This basically talks about creating.

00:04:52:15 - 00:04:53:18

Speaker 2

A cyber militia.

00:04:54:14 - 00:05:00:05

Speaker 1

And gives the requirements, the training, how people would set up.

00:05:00:05 - 00:05:03:08

Speaker 2

A cyber militia.

00:05:03:08 - 00:05:08:13

Speaker 1

Let's see if we can get a better view of it. I'll leave the link below.

00:05:08:13 - 00:05:09:18

Speaker 2

But the reason.

00:05:09:18 - 00:05:19:24

Speaker 1

Why the reason why I present this is that this kind of gives a nice overview of justifying why we would be talking about.

00:05:20:00 - 00:05:20:14

Speaker 2

Cyber.

00:05:20:14 - 00:05:26:26

Speaker 1

Militias. Okay. How people would respond in a cyber.

00:05:26:26 - 00:05:38:03

Speaker 2

Malicious sort of way. These are the courses. These are the free online courses that are available for college credit. So the paper walks you through all that.

00:05:38:03 - 00:05:40:05

Speaker 1

And you know, the paper.

00:05:40:05 - 00:05:42:01

Speaker 2

Is designed primarily for.

00:05:42:01 - 00:05:43:17

Speaker 1

A augmentation.

00:05:43:17 - 00:05:47:12

Speaker 2

Or cyber militia type operations for hospitals.

00:05:47:12 - 00:05:50:04

Speaker 1

Now, why hospitals are it when you start studying.

00:05:50:04 - 00:05:55:24

Speaker 2

Cyber militias, you're going to find out more and more they're popular to be suggested for smaller countries.

00:05:56:13 - 00:05:58:17

Speaker 1

So we have gigantic countries that can.

00:05:58:17 - 00:06:01:03

Speaker 2

Participate in cyber warfare operations fairly.

00:06:01:03 - 00:06:03:16

Speaker 1

Easily Russia, China, the United.

00:06:03:16 - 00:06:04:27

Speaker 2

States, North Korea.

00:06:04:27 - 00:06:08:21

Speaker 1

Places like that. But if you're a country caught in the crossfire.

00:06:08:21 - 00:06:09:00

Speaker 2

If you're.

00:06:09:00 - 00:06:14:01

Speaker 1

Caught in the middle, what are you going to do? You're going to have to have a.

00:06:14:07 - 00:06:15:21

Speaker 2

Cyber militia force.

00:06:16:00 - 00:06:16:25

Speaker 1

That can be quickly.

00:06:16:25 - 00:06:17:21

Speaker 2

Brought together.

00:06:18:29 - 00:06:26:24

Speaker 1

Because and this is an important phrase of going to give you right now, low probability, high impact. So even though.

00:06:26:24 - 00:06:29:24

Speaker 2

Cyber warfare and cyber attacks are low probability.

00:06:30:13 - 00:06:33:23

Speaker 1

When they do hit, they could have a high impact.

00:06:33:23 - 00:06:35:01

Speaker 2

So cyber warfare is.

00:06:35:01 - 00:07:01:18

Speaker 1

Low probability, but when it does head, it's high impact. So in a low probability, high impact arena, you have to have a response team, Where are you going to get your response team from? How have they trained? Do they know what they're doing, what's going on? So that's what this paper tries to address. So the only reason I provide that is so that people can feel a little bit of confidence that, you know, these papers have been out there, We've been putting these suggestions in front of the industry.

00:07:01:27 - 00:07:02:12

Speaker 1

People have.

00:07:02:12 - 00:07:03:13

Speaker 2

Been reviewing.

00:07:03:13 - 00:07:07:20

Speaker 1

Them. And this incident that happened with.

00:07:07:25 - 00:07:08:17

Speaker 2

George is a.

00:07:08:17 - 00:07:11:19

Speaker 1

Perfect example to start dusting some of these things off and seeing if they.

00:07:11:19 - 00:07:12:02

Speaker 2  
Work.

00:07:13:03 - 00:07:17:10

Speaker 1  
Especially in the cyber militia concept. We can't talk about this stuff anymore.

00:07:17:10 - 00:07:18:11

Speaker 2  
It's time for action.

00:07:19:09 - 00:07:21:27

Speaker 1  
So that's kind of what we're doing on this channel. That's what puts us.

00:07:21:27 - 00:07:24:13

Speaker 2  
Out in the forefront.

00:07:24:13 - 00:07:28:24

Speaker 1  
As you can see, the whole concept of the ethics of a cyber militia and.

00:07:28:24 - 00:07:39:27

Speaker 2  
How a cyber militia would operate. How does it respond to protecting critical infrastructure against cyber gangs, state actors, non-state actors, etc.?

00:07:41:06 - 00:07:44:02

Speaker 1  
I think this is fascinating. I think this.

00:07:44:02 - 00:07:45:10

Speaker 2  
Is where it's at.

00:07:46:17 - 00:07:55:17

Speaker 1  
These are the issues and the questions that have not been resolved by the military, by government, by the United Nations, by Geneva, by anybody. These questions are just sitting.

00:07:55:17 - 00:07:58:06

Speaker 2  
Out there waiting for the cyber war to kick off.

00:07:58:06 - 00:08:05:04

Speaker 1  
To see how are we going to answer these questions. So our takeaway.

00:08:05:10 - 00:08:05:26

Speaker 2

For our.

00:08:05:26 - 00:08:09:21

Speaker 1

Purposes, you can look at the paper on the, you know, the.

00:08:09:21 - 00:08:11:13

Speaker 2

Cyber first responder. If you want.

00:08:11:18 - 00:08:14:00

Speaker 1

To get an idea of what I was thinking about.

00:08:15:01 - 00:08:16:12

Speaker 2

That's more specifically.

00:08:16:12 - 00:08:22:24

Speaker 1

Related to hospital protection. But you could use the same analogy in bulk electricity.

00:08:23:09 - 00:08:27:05

Speaker 2

Protection or water and dams protection.

00:08:27:05 - 00:08:33:29

Speaker 1

You know, the list goes on. And then that's one takeaway. The second takeaway is know that Estonia in 20.

00:08:33:29 - 00:08:35:15

Speaker 2

17 is really the birth of the.

00:08:35:15 - 00:08:41:22

Speaker 1

Cyber militia and justifies the use of cyber militias, especially with smaller organizations that would be.

00:08:41:23 - 00:08:42:26

Speaker 2

Caught in the crossfire.

00:08:43:09 - 00:08:44:27

Speaker 1

Such as hospitals, such as critical.

00:08:44:27 - 00:08:46:15

Speaker 2

Infrastructure, such as ports.

00:08:47:07 - 00:08:57:18

Speaker 1

And that we have to start thinking as a nation, is this something that we need? And I say, yes, yes, yes, we need it, because the professional people just aren't up to the task.

**(EXHIBIT C)**

# **PORT OF CHARLESTON DIRTY BOMB HOAX AND SOCIAL MEDIA LIABILITY**

**“DIRTY BOMB ... PLEASE  
INVESTIGATE ... MAERSK MEMPHIS”**

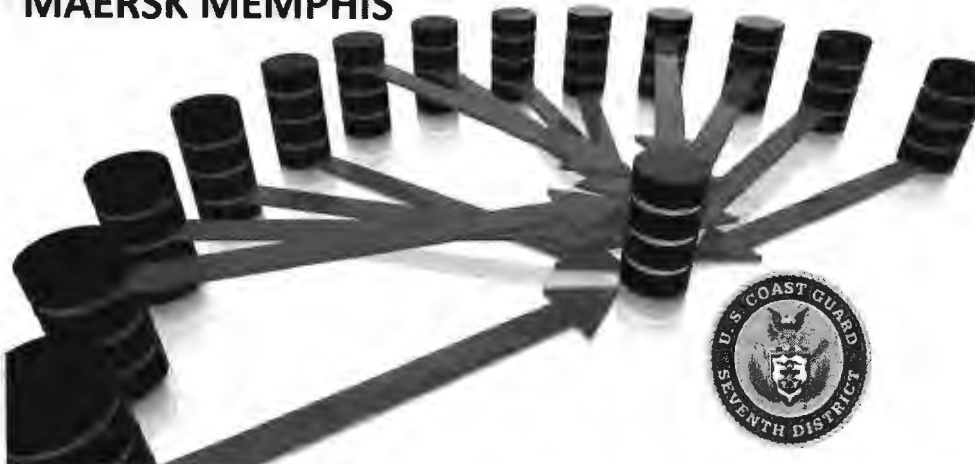




# Port of Charleston Dirty Bomb Hoax

Immediate Need for Deterrence  
Against Weaponized Deception

**DIRTY BOMB ... PLEASE INVESTIGATE ...  
MAERSK MEMPHIS**



**WARNING:** This document provides a threat assessment of a cyber-attack vector. Individuals listed in this report should not be considered guilty of any crime or offense. The focus of this document is to present evidence of the telecommunications aspects of the “dirty bomb” alert and warning received by the U.S. Coast Guard on June 14<sup>th</sup>, 2017 in the context of federal law. Any individual discussed should be presumed innocent of any crimes until adjudicated otherwise in an appropriate court of law.

DRAFT

## ***Executive Summary***

This evidentiary report places certain actions of a YouTube celebrity, who initiated a radiological event response during a hoax reality news show, within the context of federal law.

As demonstrated by the Port of Charleston “dirty bomb hoax” on June 14<sup>th</sup>, 2017, profit-motivated YouTube entertainers masquerading as legitimate news channels are now an emerging threat to the critical infrastructure operators of the United States.

This dangerous trend indicates that socially engineered public panics can be used to mask more serious simultaneous cyber-attacks (known as blended attacks).

Blended critical infrastructure attacks can be composed of (1) hoax or false **content** designed to alarm and distress, and (2) are distributed devices designed to **flood and overwhelm** the target. The goal of a blended act is to force an ill-advised **call-to-action** (CTA) upon the victim.

This type of weaponized deception is the product of supposed “crowd sourcing”. Crowd sourcing themes can drive Live Action Role Plays (**LARPs**) that offer an Augmented Reality Game (**ARG**) experience couched in the terms of “investigative journalism”.

The journalism reality show **CrowdSourceTheTruth** (CSTT) operated by Jason Goodman, convinced two (2) audience members to call the duty officer at the U.S. Coast Guard Charleston Sector with verbal information about a “dirty bomb” which led to the closure of a marine terminal in June 2017.

**Three minutes** after the initial verbal reports were telephoned to the U.S. Coast Guard Charleston Sector, CSTT’s Goodman asked his audience of over **2,000** to tweet the following message to 7<sup>th</sup> District U.S.C.G. Unified Command (resulting in a “**Twitter Storm**” of **8,000** impressions).

**“DIRTY BOMB ... PLEASE INVESTIGATE ... MAERSK MEMPHIS”**

The second warning (“Twitter Storm”) was a distributed denial of service (**DDoS**) attack that transmitted false and deceptive information to an official U.S. Government law enforcement agency.

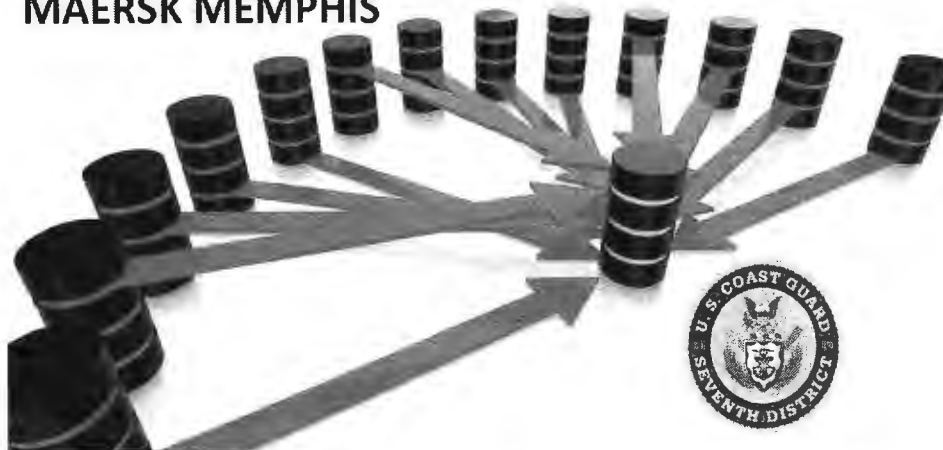
These activities appear to violate the following federal laws.

**18 U.S.C. 1038**      **CONTENT:** Goodman caused to be transmitted the following message to the 7<sup>th</sup> District Coast Guard Headquarters: **"DIRTY BOMB ... PLEASE INVESTIGATE ... MAERSK MEMPHIS"**. This content was fake and a hoax.

**18 U.S.C. 1030**      **DELIVERY:** Goodman caused the above message to be transmitted with at least 8,000 Twitter impressions in a Distributed Denial of Service (**DDoS**) attack on the 7<sup>th</sup> District U.S. Coast Guard Headquarters (Unified Command).

As depicted below, the **content** of the message ("DIRTY BOMB etc") was based on false and deceptive information. The vehicle used to transmit the message to the U.S. Coast Guard 7<sup>th</sup> District Unified Command was a **DDoS-style** attack via Twitter.

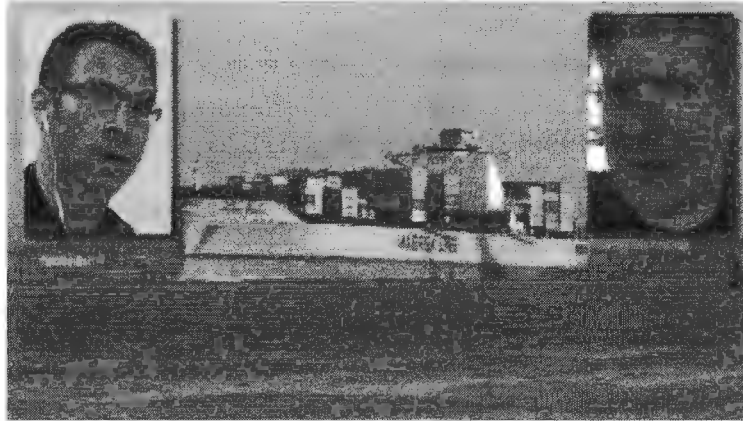
**DIRTY BOMB ... PLEASE INVESTIGATE ...  
MAERSK MEMPHIS**



## Contents

<i>Executive Summary</i> .....	3
PART I: .....	6
<i>Background</i> .....	8
<i>Weaponized Deception</i> .....	9
<i>Weak Legal Deterrence Provides Immunity to Hoax Channels</i> .....	10
PART II: .....	11
<i>Overcoming the Legal Obstacles to Prosecution</i> .....	12
<i>The Curious Deep Uranium, aka Rock Hudson of The Hudson Report</i> .....	14
PART III: .....	16
<i>Presumed Violations of Federal law</i> .....	17
PART IV: .....	19
<i>Weaponization of Attack Bots by CSTT Affiliates</i> .....	20
<i>Attack Tools Border on Cyber Warfare</i> .....	22

**PART I:  
HOAX THREAT ACTORS  
ATTACK U.S.C.G.  
7<sup>th</sup> DISTRICT**

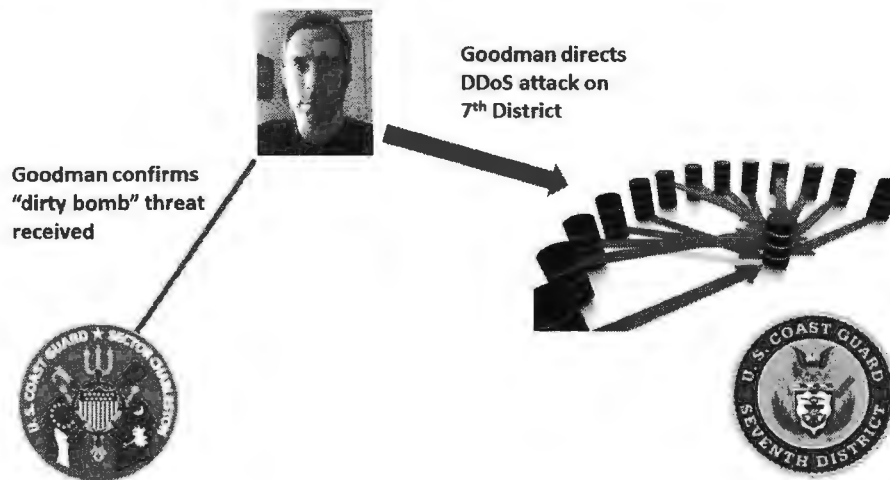


L/R: Jason David Goodman, the MAERSK MEMPHIS, George Webb Sweigert

### Three minutes between incident A and incident B

2:01:28

2:04:28



Taxonomy of distribution of dirty bomb alert and warning.

## ***Background***

No individual(s) have ever been held accountable for the social media generated public hysteria that led to the emergency closure of a marine terminal at the Port of Charleston, S.C. on June 14<sup>th</sup>, 2017.

The maritime terminal closure was based on a “dirty bomb” tip provided by individuals that supposedly had knowledge of the shipment of a weapon of mass destruction (WMD) on the **MAERSK MEMPHIS** container ship (arriving in the Port of Charleston).

Two separate incidents of “dirty bomb” warnings occurred in sequence.

### **Incident A**

Two (2) “dirty bomb” phone calls were received by the U.S. Coast Guard (U.S.C.G.) duty officer at the Charleston Sector after CSTT “intelligence coordinator” Goodman provided the emergency number live on the air (**843-740-7050**)<sup>1</sup>.

At least one of these callers was discovered to be a very close affiliate of the CSTT reality show (allegedly **Joe Napoli**).

A third call was made to the duty officer by Goodman himself to confirm that the “dirty bomb” messages were received.

Goodman (during a third call) verified (live on-air) with the duty officer at the Charleston Sector that U.S. Coast Guard Charleston Sector<sup>2</sup> that he had received the “dirty bomb” warnings.

### **THREE MINUTES TRANSPIRE**

#### **Incident B**

Three minutes after Goodman’s call to the Charleston Sector Goodman orchestrated a **DDoS** attack by suggesting everyone in his 2,117 member audience send a Twitter message to the higher command of the Charleston Sector – 7<sup>th</sup> District Unified Command. The transmission of these tweets resulted in 8,000 Twitter impressions, which flooded the 7<sup>th</sup> District with the following message.

#### **“DIRTY BOMB – PLEASE INVESTIGATE – MAERSK MEMPHIS”**

There appears to be no legitimate reason to justify the redundant DDoS “Twitter Storm”. Understandably, these messages created a panic that bordered on mass hysteria accompanied by a full-scale radiological incident response followed requiring the deployment of police, fire, EMS, public works, specialty teams, etc.

---

<sup>1</sup> <https://www.nytimes.com/2017/06/15/us/port-dirty-bomb-south-carolina.html>

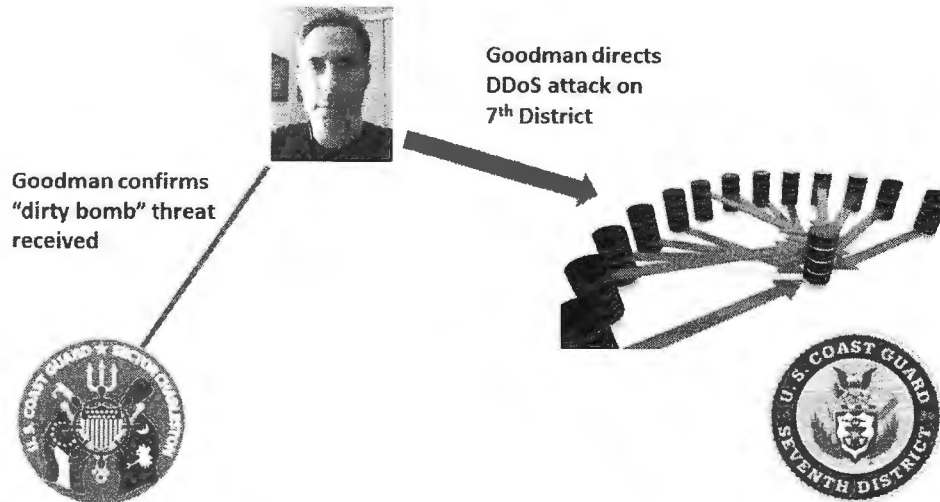
<sup>2</sup> <https://www.atlanticarea.uscg.mil/Our-Organization/District-7/Units/Sector-Charleston/>



## Three minutes between incident A and incident B

2:01:28

2:04:28



### *Weaponized Deception*

For Internet celebrities willing to create hoaxes based upon deceptive information (labeled as "news") their drama can be wrapped in an "investigative journalist" wrapper. This enables such channels to be in the center of the news, rather than merely just report the news.

CSTT hoaxes usually involve the activation of public safety resources to increase the allure of the perceived threat for the audience. This creates a strong emotional bond between the audience, actors and the storyline.

After audience members develop emotional commitment and engagement, a CSTT call-to-action (**CTAs**) is coerced from them. These CTAs may include e-mail bombing a target's mail address, calling the places of employment of targets and reporting criminal investigations, inciting acts of retribution against targets perceived as "enemies of the truth", etc.

Theatrical presentations of "nerve centers" (like CSTT) can bring an audience to an enhanced climax based on the inducement of fear. This can be likened to the Orson Wells broadcast of "War of the Worlds" in 1938. Such reality shows, also known as Live Action Role Plays (**LARP**), include the injection of periodic "intelligence reports" from "inside sources" to create an Augmented Reality Game (**ARG**).

These same threat actors (CSTT + CSTT affiliates) have recently increased their threat capability by operationalizing technical “attack bots” designed to automatically broadcast false information when a certain set of circumstances triggers their logic. These bots can be deployed to create “Twitter Storms” similar to Charleston.

CSTT threat actors have openly stated their desire to attack critical infrastructure to “crash the machine” and “reset the system” as part of an Internet doomsday cult philosophy<sup>3</sup>. Operationalized attack auto-bots factor heavily into this philosophy. This is not a fanciful and harmless threat.

The lack of criminal prosecution of these threat actors has created a fertile environment for continued testing and prototyping of these hoax enhancing auto-bots.

### ***Weak Legal Deterrence Provides Immunity to Hoax Channels***

Laws and policies only deter if three conditions are present:

- Fear of penalty
- Probability of being caught
- Probability of penalty being administered

No deterrence has been undertaken to mitigate these CSTT hoax threat actors from creating more hoaxes impacting public safety. Since Charleston copy-cat hoax events have been staged in New Mexico by the same profit-driven threat actors (claiming an assassination attempt made on a CSTT “reporter”).

These repeated public safety hoaxes appear to be an act of perfecting their hoax attack methods. There is a definite and well documented life cycle to the hoaxes created by “CSTT” to generate views and profits.

This type of threat to critical infrastructure has yet to be addressed firmly with legal action. Thus, a deterrence capability is lacking. Without effective deterrence, others (motivated by profit) will stage similar hoaxes.

---

<sup>3</sup> See #TeamTyler and Project Mayhem operated by Quinn Michaels

**PART II:**  
**WILLFUL BLINDNESS OF CSTT**

### ***Overcoming the Legal Obstacles to Prosecution***

CSTT hoax threat actors are fond of relying on their willful blindness and conscious disregard to apparent common sense, facts and contradictory information as an immunity defense.

The consistent reliance on ignorance to certain facts is an example of willful recklessness to avoid the truth. CSTT affiliates deliberately feign ignorance and practice avoidance of the actual circumstances surrounding these hoax events.

#### **Willful blindness in a criminal context**

**Example:** When a drug transport smuggler (“mule”) crosses the U.S.-Mexican border they can claim s/he was not aware of the 162 pounds of marijuana in the car’s secret compartment. This willful ignorance defense does not work.

In the same manner, when profit-motivated hoax threat actors forwards unvented warnings (“dirty bomb”) to law enforcement<sup>4</sup> (understanding the consequences of such information) and then claims ignorance of the consequences (“I trusted the source”) it represents a fact pattern as described in United States v. Jewell, 532 F.2d 697 (9th Cir. 1976):

*"One with a deliberate antisocial purpose in mind . . . may deliberately 'shut his eyes' to avoid knowing what would otherwise be obvious to view. In such cases, so far as criminal law is concerned, the person acts at his peril in this regard, and is treated as having 'knowledge' of the facts as they are ultimately discovered to be."*<sup>5</sup>

Goodman’s own words demonstrate the concept. In the following show excerpt, Mr. Goodman speaks about the trust he has placed in someone called “Deep Uranium” (later discovered to be a former FBI informant) as source the “dirty bomb” warnings.

Recall **Incident A** when Mr. Goodman verified via phone call that the duty officer at the U.S.C.G. Sector Charleston had received a “dirty bomb” threat. Then the following remarks are made by Goodman on video, immediately following confirmation of the “dirty bomb” warning.

---

<sup>4</sup> <https://law.justia.com/cases/federal/appellate-courts/F2/532/697/99156/>

<sup>5</sup> R. Perkins, Criminal Law 776 (2d ed. 1969)

*"...We've received information from a person known to me through George (Webb) as someone who is in the law-enforcement community or the whatever intelligence community. I don't know this person but I know that George frequently tells me he's spoken to this person . . . George tells me he's spoken to this person and such and is going to happen and then ... more than once the person was correct."* 2:30:20 of video<sup>6</sup>. Remarks of Jason Goodman on 6/14/2017 YouTube reality show "CSTT".

Recall **Incident B** when Mr. Goodman requested **2,117** audience members tweet "DIRTY BOMB – PLEASE INVESTIGATE – MAERSK MEMPHIS" to the 7<sup>th</sup> District Unified Command (resulting in 8,000 Twitter impressions).

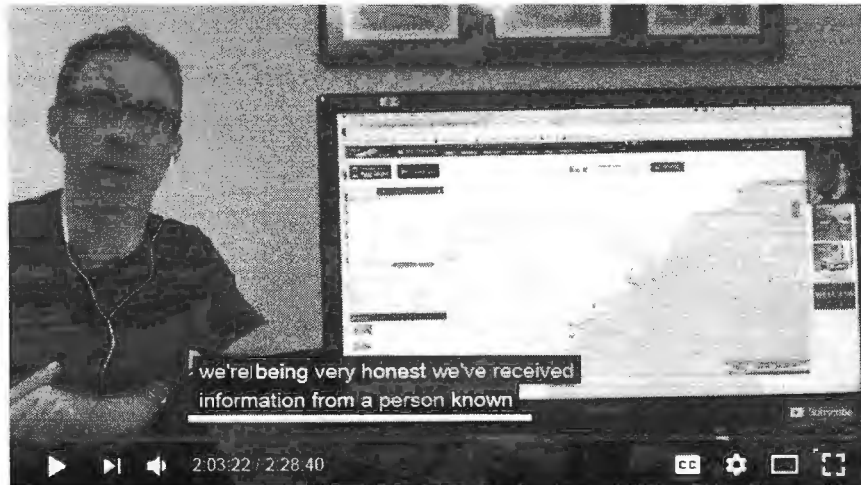
However, an hour prior to these events Goodman telephone intelligence analyst and author Dr. Jermon Corsi<sup>7</sup> to seek his advice and consultation.

**01:09:42** Jason Goodman contacts Corsi to inquire about the threat

**01:17:15** Corsi responds he doesn't know anything about the threat

**01:20:51** Corsi re-iterates he cannot corroborate anything about the threat

**01:41:06** Corsi repeats again he has ZERO confirmation of the threat



Clear and Present Danger (Calm Before the Storm?) #maerskmemphis

Video of CSTT, Jason Goodman owner/operator

<sup>6</sup> <https://www.youtube.com/watch?v=ekr5cw2WAbU&t=7799s>

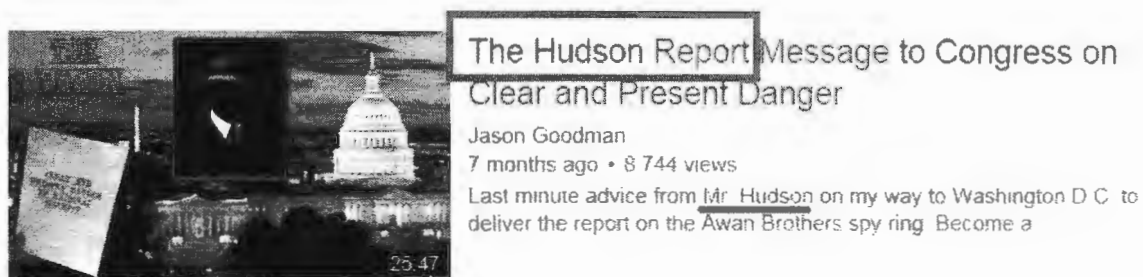
<sup>7</sup> <http://www.simonandschuster.com/authors/Jerome-R-Corsi/48217651>



This information from an intelligence industry analyst and “insider” was subsequently disregarded by Goodman.

In sum, Mr. Goodman proceeded at his own peril and risk to broadcast the fake hoax threat to the 7<sup>th</sup> District Unified Command (**Incident B**) based on vague and ambiguous knowledge of a mystery man known as “Deep Uranium”.

The source of this dirty bomb “intelligence” (“Deep Uranium”) is a former FBI informant. It is very telling that a few weeks after the 6/14/2017 Port of Charleston incident, Mr. Goodman inaugurated a special CSTT exclusive weekly feature known as the **Hudson Report** featuring “Deep Uranium” on August 14, 2017.



Screen capture of The Hudson Report

***The Curious Deep Uranium, aka Rock Hudson of The Hudson Report***  
The identity of the curious “Deep Uranium” appears to be that of a former FBI informant living in West Virginia.



The likely individual known as Deep Uranium and Rock Hudson on CSTT<sup>8</sup>

<sup>8</sup> <https://www.youtube.com/watch?v=zsSZ-NC8ils>

## **Militia leader guilty in bomb plot**

**Aug. 8, 1997**

**WHEELING, W.Va.** -- The self-proclaimed general of West Virginia's Mountaineer Militia has been convicted of plotting to blow up the FBI's fingerprint laboratory. A U.S. District Court jury found Floyd 'Ray' Looker, a Vietnam veteran who lives in Stonewood, W.Va. and claims to be a gospel preacher, guilty of conspiracy to engage in manufacturing and dealing in explosives without a license.

The 56-year-old Looker, who testified in his own behalf Thursday, had told jurors he didn't know it was illegal to build bombs. He said he wanted to stockpile explosives in case the United States were invaded by a foreign force. The government, however, said Looker planned to use the explosives to blow up the FBI's fingerprint lab in Clarksville, W.Va., about 90 miles south of Pittsburgh. Looker was arrested Oct. 11, 1995 after he allegedly sold blueprints of the FBI fingerprint complex for \$50,000 to an undercover agent who claimed to represent a terrorist group. The prosecution's case was based information received from a former militia member who has since entered the government's witness protection program. The informant, **Okey**

**Marshall Richards Jr.**, made more than 400 tape recordings that led to the arrest of Richards. Defense attorneys called Richards' two ex-wives who told the court the informant is a pathological liar. The two women also said he owed them at least \$40,000 in alimony and child support. Looker's co-defendants, Jack Arland Phillips and Edward F. Moore, both entered guilty pleas at earlier hearings.

The Hudson Report was marketed by CSTT as an "intelligence report", including a synopsis of leaked law-enforcement and/or intelligence community information. The focus of The Hudson Report was to create drama and interest based on upcoming events related to "intelligence assessments".

This was a regular feature of CSTT; the showcasing of the same individual who was the alleged source of the "dirty bomb" threat information.

**PART III:  
SUFFICIENCY OF  
LEGAL REMEDIES**



## *Presumed Violations of Federal law*

### **18 U.S.C. § 1030, COMPUTER FRAUD AND ABUSE ACT**

18 U.S.C. § 1038 states:

(5)

(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

In 2011, the Sixth Circuit Court of Appeals addressed similar DDOS-style attacks in Pulte Homes, Inc. v. Laborers' Intern. Union of North America, 648 F.3d 295 (6th Cir. 2011).

This case that did not deal directly with a per se **DDoS** attack but did deal with a labor union's concerted email and telephone "attack" on a company of such a volume that it disrupted the company's ability to do business<sup>9</sup>.

The issue before the court in *Plute* was whether the labor union "intentionally caused damage" by causing e-mail bombs and needless phone calls to a business. The Pulte Court, in finding a violation of the Computer Fraud and Abuse Act and, consequentially, "damage" arising from this activity, held that "a transmission that weakens a sound computer system—or, similarly, one that diminishes a plaintiff's ability to use data or a system" causes damage. *Id.* at 301. The court reasoned:

Under the **CFAA**, "any impairment to the integrity or availability of data, a program, a system, or information" qualifies as "damage." Because the statute includes no definition of three key terms—"impairment," "integrity," and "availability"—we look to the ordinary meaning of these words. "Impairment" means a "deterioration" or an "injurious lessening or weakening." The definition of "integrity" includes an "uncorrupted condition," an "original perfect state," and "soundness." And "availability" is the "capability of being employed or made use of." Applying these ordinary usages, we conclude that a transmission that weakens a sound computer system—or, similarly, one that diminishes a Plaintiff's ability to use data or a system—causes damage."

---

<sup>9</sup> <https://shawnetuma.com/2013/10/09/yes-case-law-says-it-really-is-a-cfaa-violation-to-ddos-a-website/>

## 18 U.S.C. § 1038, TERRORIST HOAX IMPROVEMENTS ACT OF 2007

18 U.S.C. § 1038 states:

**(a) Criminal Violation.—**

**(1) In general.—Whoever engages in any conduct with intent to convey false or misleading information under circumstances where such information may reasonably be believed and where such information indicates that an activity has taken, is taking, or will take place that would constitute a violation of [specified anti-terrorism laws,] shall [be fined or imprisoned as provided].**

In 2017, a 21 y.o. volunteer fire fighter in Columbia, S.C. was sentenced to one year of imprisonment and three years of supervised probation for phone texting three unknown people that he had heard that someone placed a bomb at a Veteran's Administration Medical Center<sup>1</sup>.

As suggested in *United States v. Jewell*, 532 F.2d 697 (9th Cir. 1976), Mr. Goodman's willful blindness to the sources of the 6/14/2017 dirty bomb warnings (calculated to cause panic and disrupt the civil peace) does not provide an adequate defense.

To address the intent requirement of 18 U.S.C. 1038 it is instructive to note the wisdom of *United States v. Castagana*, 604 F.3d 1160, 1164 (9th Cir. 2010).

*Whether the circumstances were such that Castagana's victims or other observers may reasonably have believed his statements to indicate terrorist activity is a question wholly independent of Castagana's intentions. That is precisely what a reasonableness standard, triggered by factual circumstances, means. The insertion of this reasonableness requirement removes from consideration the subjectivity of the actor's intent and replaces it with an objective standard.*

The intention of Mr. Goodman is not an issue. The willful blindness on Goodman's part to seize on "intelligence" information from a former FBI informant to create a Twitter Storm is the issue.

**PART IV:  
BURGEONING CAPABILITIES  
OF  
CSTT THREAT ACTORS**

### ***Weaponization of Attack Bots by CSTT Affiliates***

Cognitive (mind) threats are a type of social engineering attack that demands immediate action based on a perceived crisis (always based on deception). For such attacks to work there must be an appearance of legitimacy ("intelligence source"). E-mail phishing attacks are an example of deception based social engineering designed for an illegitimate call to action.

These attacks (like **Incident B**) can overwhelm public safety responders in an instant, sewing confusion which blurs proper situational awareness and threat assessment.

The speed of the Internet, the large audience reach of social media platforms, and the opportunity to fashion hoax events create attacks that are largely unknown and unfamiliar to public safety responders.

Deception coupled with "auto bot" or "bot" technology is even more troubling. The same CSTT group responsible for Charleston is perfecting a type of "doomsday" auto-bot messaging system with the end objective to "reset the machine".

These CSTT affiliates (emboldened by the lack of a legal threat) are openly communicating via YouTube and Twitter to create a Project Mayhem type of doomsday network. This is a recipe for a larger scale hoax in the future.

The auto-bot network can (labeled #TimePhoneHack) disseminate massive disinformation via social media networks to create panic in seconds. The same CSTT threat actors involved Charleston are now using sophisticated Artificial Intelligence (AI) techniques to perfect their methods (in plain view).

### Time Phone Hack #tyler #teamtyler - YouTube

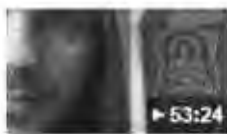


<https://www.youtube.com/watch?v=Q5B6OZInPTU>

4 days ago - Uploaded by quinn michaels

Developing artificial intelligence with a unique perspective. Quinn Michaels is working on Indra.ai an artificial ...

### Time Phone Hack #Tyler #TeamTyler - YouTube



<https://www.youtube.com/watch?v=3jy8xc02aH8>

4 days ago - Uploaded by quinn michaels

Developing artificial intelligence with a unique perspective. Quinn Michaels is working on Indra.ai an artificial ...

### Time Phone Hack How To Hack Time - YouTube



<https://www.youtube.com/watch?v=n4e481lAsbo>

1 day ago - Uploaded by quinn michaels

Developing artificial intelligence with a unique perspective. Quinn Michaels is working on Indra.ai an artificial ...

### Time Phone Hack And Were Back - YouTube

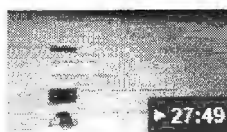


[https://www.youtube.com/watch?v=LvSI7-ab\\_Sk](https://www.youtube.com/watch?v=LvSI7-ab_Sk)

1 day ago - Uploaded by quinn michaels

Developing artificial intelligence with a unique perspective. Quinn Michaels is working on Indra.ai an artificial ...

### Time Phone Hack More Entertaining - YouTube



<https://www.youtube.com/watch?v=ZNvJ56T8Ktk>

3 days ago - Uploaded by quinn michaels

Developing artificial intelligence with a unique perspective. Quinn Michaels is working on Indra.ai an artificial ...

### ***Attack Tools Border on Cyber Warfare***

Cognitive attacks (weaponized deception) coupled with technology devices (auto-bots) have created a new style of cyber threat known as blended attacks. Such attacks are multi-layered and can avoid traditional pre-attack indicators. Techniques such as these are bordering on the domain of cyber warfare.

The sophistication of this style of attack will remain perplexing to traditional first responder resources (as with Charleston). As this paper is being written, a bot-net style attack apparently launched by CSTT is presently underway.

The CSTT affiliate known as “Quinn Michaels” is presently openly recruiting followers to launch cyber-based attacks in the perceived enemies and rivals of CSTT. Michaels, who claims to understand the Palantir<sup>10</sup> intelligence algorithms, is engineering an Artificial Intelligence (A.I.)-based bot network to monitor social media for trigger words and respond with replies to guide and enhance a cognitive attack.

These attacks indicate that the CSTT confederation have not been deterred by the closure of the Port of Charleston and the downstream consequences of that event. In fact, the opposite is true – they have become embolden by the lack of legal accountability.

This type of threat to critical infrastructure has yet to be addressed firmly with legal action. Thus, a deterrence capability is lacking. Without effective deterrence, others (motivated by profit, philosophy, ideologies, etc.) will stage similar hoaxes.

Meanwhile, the lack of criminal prosecution of these threat actors has created a fertile environment for testing and prototyping hoax enhancing auto-bots.

---


<sup>10</sup> <https://www.bloomberg.com/features/2018-palantir-peter-thiel/>

## **ANNEX**

**Dr. Jermone Corsi (consulted one hour before Incident B)**

File Edit View Favorites Tools Help

Not logged in Talk Contributions Create account Log



**WIKIPEDIA**  
The Free Encyclopedia

Main page  
Contents  
Featured content  
Current events  
Random article  
Donate to Wikipedia  
Wikipedia store  
  
Interaction  
Help  
About Wikipedia  
Community portal  
Recent changes  
Contact page  
  
Tools  
What links here  
Related changes  
Upload file  
Special pages  
Permanent link  
Page information  
Wikidata item  
Cite this page  
  
Print/export  
Create a book  
Download as PDF  
Printable version  
  
In other projects  
Wikiquote

Article Talk

Read Edit View history

## Jerome Corsi

From Wikipedia, the free encyclopedia

**Jerome Robert Corsi** (born August 31, 1946) is an American author, political commentator, and conspiracy theorist<sup>[3][4]</sup> best known for his two *New York Times* Best Selling books: *The Obama Nation* and *Unfit for Command* (with co-author John O'Neill). Both books, the former written in 2008 and the latter in 2004, attacked Democratic presidential candidates and were criticized for including numerous inaccuracies.<sup>[5][6][7]</sup>

In other books and columns for conservative sites such as *WorldNetDaily* and *Human Events*, Corsi has discussed topics that are considered conspiracy theories, such as the alleged plans for a North American Government, the theory that President Barack Obama is not a United States citizen,<sup>[8]</sup> criticism of the United States government for allegedly covering up information about the terrorist attacks of September 11, 2001,<sup>[9]</sup> and alleged United States support of Iran in its attempts to develop nuclear weapons.<sup>[10][11][12]</sup>


In 2017, he became the Washington, D.C. bureau chief for the conspiracy theory website *InfoWars*.

Contents [hide]

1 Early life and education
2 Career
3 Writings and conspiracy theories

3.1 *Unfit for Command*
3.2 *The Obama Nation*
3.3 *Black Gold Stranglehold*
3.4 *Atomic Iran*
3.5 *Where's the Birth Certificate?*

Jerome Corsi



Corsi in 2018

**Born**

Jerome Robert Corsi  
August 31, 1946 (age 71)  
East Cleveland, Ohio, U.S.

**Residence**

Denville Township, New Jersey, U.S.

**Nationality**

American

**Education**

Case Western Reserve University (BA)  
Harvard University (PhD)  
[1]

**Occupation**

Writer

**Employer**

InfoWars<sup>[2]</sup>

**Known for**

Co-author of *Unfit for Command*, author of *The Obama Nation*

**Title**

DC bureau chief<sup>[2]</sup>

**Political**

Constitution Party



**“Rock Hudson” discusses the Port of Charleston in an August 14, 2017 video<sup>11</sup>.**



### Hudson Revealed



Jason Goodman



19,801 views



Published on Aug 14, 2017

*“In regards to **George Webb** I have a tremendous respect for Webb and I don’t mind telling you –*

*and that is that **George is just an amazing** – that you what a mind -- yeah – what a mind – I can’t speak enough of it, I mean it’s just ....*

*You take for example intelligence and people say well how do we know this guy [Hudson] is telling us the truth – well okay ...*

*We know, we know for a fact that **425 million cargo containers** are transported each year in the world that represents over 90 percent of the world’s total trade ...*

***Charleston South Carolina is a port hub** – those hubs – depending on the security protocols that their using – that day or that shift – they can process 1,500 to **50 thousand** containers per day. That raised an eyebrow with me...*

*But, don’t worry because they really do care about you ...*

***They should be ashamed of themselves** ...” Beginning at 39:20 in the YouTube video “Hudson Revealed” published August 14, 2017.*

---

<sup>11</sup> <https://www.youtube.com/watch?v=TWUI8gDPFx0&t=2021s>


**Goodman provides recap of the dirty bomb hoax at 1:33, names Joe Napoli at 3:13, continues on to 8:51**



Unrig Cynthia McKinney



Jason Goodman

 Subscribe 58K

11,504 views

 Like  Share  More

 273  10

[https://www.youtube.com/watch?v=tSI0ZflsN\\_k](https://www.youtube.com/watch?v=tSI0ZflsN_k)

### Example of the weekly "The Hudson Report" YouTube shows



#### Hudson Report - Benjamin Paddock & Battlefield Las Vegas

Jason Goodman  
5 months ago • 23,870 views

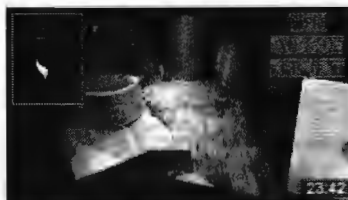
Become a sponsor of Crowdsorce the Truth and support the effort  
<http://paypal.me/crowdsourcethetruth> <https://www.patreon.com/>



#### Hudson Revealed

Jason Goodman  
8 months ago • 19,783 views

With over 40 years of military, intelligence and clandestine experience, confidential Crowdsorce operative codename HUDSON



#### The Hudson Report - Multiple Shooters in Las Vegas?

Jason Goodman  
8 months ago • 16,933 views

Mr. Hudson provides his analysis that indicates multiple shooters, multiple rates of fire and multiple caliber weapons. Become a



#### Hudson Report Awan Bros IT Scandal Hearing

Jason Goodman  
6 months ago • 10,510 views

Mr. Hudson returns after being off grid for several days on a recon mission. He weighs in on the Las Vegas massacre, Tom Fitton's



#### Hudson Report - Criminal Congress

Jason Goodman  
6 months ago • 8,680 views

Mr. Hudson continues to name names in the time and manner of his choosing as he enumerates a stunning historical list of

---

<sup>i</sup> <https://www.justice.gov/usao-sc/pr/columbia-man-sentenced-making-hoax-bomb-threat>



71911657R00018

Made in the USA  
Middletown, DE  
01 May 2018



The next generation of cyber warfare attack tools will be based upon Artificial Intelligence. A.I. tools can execute complex social media attacks to create panic. Law enforcement is falling further behind the tip of the spear in comprehending the cyber warfare nature of these attack techniques.

This booklet describes how social media hoax news sites can attack America's critical infrastructure. Seemingly, these deception merchants operate with no threat of legal action. This fertile environment has allowed the consequence-free attacks on maritime ports, generation of hysteria of supposed assassination plots, etc.

The alleged deception merchant described herein is Jason David Goodman of New York City, operator of the "business" CrowdSourceTheTruth (a social media conspiracy channel).

**WARNING:** No individuals described herein should be presumed to be guilty of any particular violation of law, policy or regulation. All parties should be presumed innocent until a competent court deems otherwise.



**(EXHIBIT D)**



June 7, 2022

**VIA ELECTRONIC TRANSMISSION**

The Honorable Alejandro N. Mayorkas  
Secretary  
U.S. Department of Homeland Security

Dear Secretary Mayorkas:

Department of Homeland Security (DHS) information obtained by our offices through protected whistleblower disclosures raises serious concerns about DHS's recently-paused Disinformation Governance Board (DGB) and the role the DGB was designed to play in DHS counter disinformation efforts. Documents show that, contrary to your May 4, 2022, testimony before the Senate Committee on Homeland Security and Governmental Affairs, the DGB was established to serve as much more than a simple "working group" to "develop guidelines, standards, [and] guardrails" for protecting civil rights and civil liberties.<sup>1</sup> In fact, DHS documents show that the DGB was designed to be the Department's central hub, clearinghouse and gatekeeper for Administration policy and response to whatever it happened to decide was "disinformation."

Specifically, documents describe a prominent DGB designed to "serve as the departmental forum for governance of DHS policies, plans, procedures, standards, and activities" pertaining to what the government refers to as "mis-, dis-, and mal- information," or "MDM," "that threatens homeland security" as well as the Department's internal and external point of contact for coordination with state and local partners, non-governmental actors, and the private sector.<sup>2</sup> Internal DHS memoranda also show that in practice, the DGB was expected to function as a "coordination and deconfliction mechanism... conven[ing] to discuss threats, assessments, response actions, and engagements as often as warranted."<sup>3</sup> According to the DGB's charter,

---

<sup>1</sup> Resources and Authorities Needed to Protect and Secure the Homeland: Hearing before the Senate Committee on Homeland Security and Governmental Affairs, 117<sup>th</sup> Congress (May 4, 2022).

<sup>2</sup> DHS Disinformation Governance Board Charter (February 24, 2022); The Cybersecurity & Infrastructure Security Agency (CISA), one of nine DHS components with representation on the DGB, defines misinformation as "false, but not created or shared with the intention of causing harm." CISA defines disinformation as "deliberately created to mislead, harm, or manipulate a person, social group, organization, or country," and it defines malinformation as "based on fact, but used out of context to mislead, harm, or manipulate." Cybersecurity & Infrastructure Agency, "MIS, DIS, MALINFORMATION", available at <https://www.cisa.gov/mdm>.

<sup>3</sup> "Ukraine MDM Playbook Version 12, as of 2/14/2022" at 2. See also DHS Disinformation Governance Board Charter (February 24, 2022).

Secretary Mayorkas

June 7, 2022

Page 2 of 5

“DHS-wide or Component specific proposals for funding related to efforts to counter MDM” were also required to be “appropriately coordinated with the Board, including in advance of submitting any final funding proposals.”<sup>4</sup>

While DHS components apparently have established methods for defining and analyzing disinformation, and would continue to carry out all of their normal operational functions under a DGB, it appears that the DGB was equipped to review evidence presented by representatives of the various components and guide DHS counter disinformation efforts.<sup>5</sup> A September 13, 2021, memo prepared in part by Robert Silvers, Under Secretary for Strategy, Policy, and Plans and, according to whistleblower allegations, one of two intended co-chairs of the DGB, outlined specific policy recommendations that should guide DHS efforts to counter disinformation.<sup>6</sup> The memo states that DHS’s “role in responding to disinformation should be limited to areas where there are clear, objective facts.”<sup>7</sup> It is unclear how DHS defines “clear, objective facts,” and it is unclear what safeguards, if any, DHS has put in place to ensure that individuals charged with determining which issue areas have “clear” and “objective facts” are not influenced by their own ideological and political beliefs. While the memo boldly asserts that the Department’s “counter-disinformation mission, including the choices as to what issue areas to focus on, must not be politicized and must be protected from perceptions of politicization,” some of the examples of disinformation given in the memo relate not only to foreign disinformation but issues that have been at the heart of domestic political discourse for the past several years.<sup>8</sup> For instance, the memo refers to “[c]onspiracy theories about the validity and security of elections” and “[d]isinformation related to the origins and effects of COVID-19 vaccines or the efficacy of masks.”<sup>9</sup>

Given the significant coordinating role the Department envisioned for the DGB, the consequences of installing Nina Jankowicz, a known trafficker of foreign disinformation and liberal conspiracy theories, as the DGB’s first Executive Director, would have been a disaster. Jankowicz once asserted that the Hunter Biden laptop should be viewed as a “Trump campaign product.”<sup>10</sup> Content on the Hunter Biden laptop has since been verified by multiple major news outlets.<sup>11</sup> In 2016, Jankowicz also sent out multiple tweets spreading the now-debunked claim

---

<sup>4</sup> “DHS Disinformation Governance Board Charter” (February 24, 2022) at 4.

<sup>5</sup> “DHS Disinformation Governance Board Charter” (February 24, 2022); *See also* “Ukraine MDM Playbook Version 12, as of 2/14/2022” at 2, 18.

<sup>6</sup> “DHS Disinformation Governance Board Charter” (February 24, 2022); Memorandum from Robert Silvers, Under Secretary, Office of Strategy, Policy, and Plans, and Samantha Vinograd, Senior Counselor for National Security, Office of the Secretary, for the Secretary (September 13, 2021).

<sup>7</sup> Memorandum from Robert Silvers, Under Secretary, Office of Strategy, Policy, and Plans, and Samantha Vinograd, Senior Counselor for National Security, Office of the Secretary, for the Secretary (September 13, 2021).

<sup>8</sup> *Id.*

<sup>9</sup> *Id.*

<sup>10</sup> Callie Patteson, “Ex-Disinformation Board chief Nina Jankowicz breaks silence, cites death threats” (May 19, 2022), available at <https://nypost.com/2022/05/19/ex-disinformation-board-chief-nina-jankowicz-breaks-silence/>.

<sup>11</sup> Craig Timberg, Matt Viser, and Tom Hamburger, “Here’s how The Post analyzed Hunter Biden’s laptop,” *The Washington Post* (March 30, 2022), available at <https://www.washingtonpost.com/technology/2022/03/30/hunter->



Secretary Mayorkas

June 7, 2022

Page 3 of 5

that President Trump had a “secret server” to communicate with Kremlin-linked Alfa Bank.<sup>12</sup> In 2020, Jankowicz tweeted that a podcast by Christopher Steele, the author of the debunked Steele Dossier containing Russian disinformation, had provided “some great historical context about the evolution of disinfo.”<sup>13</sup> So this begs the question, if the (former) Executive Director of the DGB is incapable of determining what is and is not disinformation, how could the DGB ever have expected to function properly under her leadership? We believe that Congress and the American people require full transparency regarding the DGB’s creation as well as the role Jankowicz would have played had she remained in her position at DHS. Toward that end, we are releasing documents we have collected during our investigation as an attachment to this letter.

Documents also suggest that the Department has been working on plans to “operationalize” its relationships with private social media companies to implement its public policy goals.<sup>14</sup> For example, we obtained draft briefing notes prepared for a scheduled April 28, 2022, meeting between Robert Silvers and Twitter executives Nick Pickles, Head of Policy, and Yoel Roth, Head of Site Integrity. The notes are marked “TBC,” and it is unclear whether the scheduled meeting actually took place. The briefing notes frame the planned meeting between Silvers and the Twitter executives as “an opportunity to discuss operationalizing public-private partnerships between DHS and Twitter, as well as [to] inform Twitter executives about DHS work on MDM, including the creation of the Disinformation Governance Board and its analytic exchange...”<sup>15</sup> According to whistleblower allegations, Nina Jankowicz may have been hired because of her relationship with executives at Twitter. Consistent with these allegations, Silvers’ briefing notes state that both Pickles and Roth know Jankowicz.<sup>16</sup> A recent DHS strategy document further discusses efforts to “[e]mpower partners to mitigate MDM threats.”<sup>17</sup> The document states that in certain cases, federal, state, local, tribal, and territorial or nongovernmental partners “may be better positioned to mitigate MDM Threats based on their capabilities and authorities.”<sup>18</sup> DHS theorizes that “[b]y sharing information, DHS can empower these partners to mitigate threats such as providing information to technology companies enabling them to remove content at their discretion and consistent with their terms of service.”<sup>19</sup>

---

[biden-laptop-data-examined/](#); Katie Benner, Kenneth P Vogel and Michael S. Schmidt, “Hunter Biden Paid Tax Bill, but Broad Federal Investigation Continues,” *The New York Times* (March 16, 2022), available at <https://www.nytimes.com/2022/03/16/us/politics/hunter-biden-tax-bill-investigation.html>.

<sup>12</sup> Jankowicz, Nina [@wicsipedia]. “Trump had not one, but two secret email servers to communicate w/ influential Russian bank. Unbelievable.” *Twitter* (November 1, 2016), available at

<https://twitter.com/wiczipedia/status/793329082167619584>; Jankowicz, Nina [@wicsipedia]. “Husband texted me ‘you have news to wake up to.’ Never thought it would be this. Confirms our worst fears about Trump. I am horrified.” *Twitter* (November 1, 2016), <https://twitter.com/wiczipedia/status/793322439505772544>.

<sup>13</sup> Jankowicz, Nina [@wicsipedia]. “Listened to this last night- Chris Steele (yes THAT Chris Steele) provides some great historical context about the evolution of disinfo. Worth a listen” *Twitter* (August 7, 2020), available at <https://twitter.com/wiczipedia/status/1291692143262814209>.

<sup>14</sup> Draft Briefing Notes, Twitter (April 28, 2022).

<sup>15</sup> *Id.*

<sup>16</sup> *Id.*

<sup>17</sup> “Ukraine MDM Playbook Version 12, as of 2/14/2022” at 17.

<sup>18</sup> *Id.*

<sup>19</sup> *Id.*

Secretary Mayorkas

June 7, 2022

Page 4 of 5

Collectively, whistleblower allegations and the documents we've reviewed raise concerns that DHS could be seeking an active role in coordinating the censorship of viewpoints that it determines, according to an unknown standard, to be "MDM" by enlisting the help of social media companies and big tech. The DGB's charter also specifically states that the DGB should "serv[e] as the Department's internal and external point of contact for coordination with state, local, tribal, and territorial partners, the private sector, and nongovernmental actors regarding MDM."<sup>20</sup>

The First Amendment of the Constitution was designed precisely so that the government could not censor opposing viewpoints – even if those viewpoints were false. DHS should not in any way seek to enlist the private sector to curb or silence opposing viewpoints. It is therefore imperative for DHS to provide additional clarity regarding its policies and procedures for identifying and addressing "MDM," as well as its efforts to "operationalize" public-private partnerships and the steps it is taking to ensure that it does not infringe on the constitutional rights of American citizens.

In order for us to better understand the role of the DGB and DHS's efforts to counter disinformation, we ask that you respond to the following no later than June 21, 2022.

1. Has DHS at any point in time asked or suggested to Twitter, Facebook, TikTok, or any other social media executives that they should censor, flag, add context to, or remove any social media posts that it believes to be disinformation?
2. Has DHS at any point in time asked or suggested to Twitter, Facebook, TikTok, or any other social media executives that they suspend or ban the account(s) of individuals believed to be promoting information it believes to be disinformation?
3. Please provide all documents, including all written and electronic communications, memoranda, and organizational documents, related to the DGB from the point that DHS first considered establishing a DGB until the present.
4. Please provide all documents, including all written and electronic communications and memoranda, related to Nina Jankowicz's selection as Executive Director of the DGB.
5. Please explain why, in your public statements and testimony before Congress, you have not fully explained the key role that the DGB was designed to play in coordinating among DHS components and engaging the assistance of the private sector.

---

<sup>20</sup> "DHS Disinformation Governance Board Charter" (February 24, 2022) at 3.

Secretary Mayorkas

June 7, 2022

Page 5 of 5

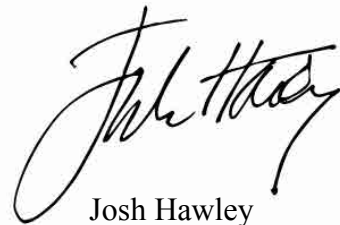
6. Please explain how DHS defines “MDM” and how DHS decides whether a given news story or other piece of information fits its definition of “MDM.” Please identify who exactly is ultimately responsible for making this determination.
7. Please explain the criteria DHS uses when deciding whether to spend taxpayer resources addressing a particular news item or narrative that it has classified as “MDM.”
8. Please describe all safeguards that DHS has put in place to ensure that its efforts to counter the spread of disinformation do not infringe on Americans’ constitutional right to free speech.
9. Did DHS Under Secretary for the Office of Strategy, Policy, and Plans Robert Silvers meet with Twitter executives on April 28, 2022? If so, please provide a summary of topics discussed during the meeting.
10. Please define what DHS means by the phrase, “operationalizing public-private partnerships.”

Thank you for your prompt attention to this important matter.

Sincerely,



Charles E. Grassley  
U.S. Senator



Josh Hawley  
U.S. Senator

Enclosures.

PRE-DECISIONAL/DELIBERATIVE

~~UNCLASSIFIED // FOR OFFICIAL USE ONLY~~

U.S. Department of Homeland Security  
Washington, DC 20528



**Homeland  
Security**

September 13, 2021

**INFORMATION**

**MEMORANDUM FOR THE SECRETARY**

**FROM:** Robert Silvers /s/  
Under Secretary  
Office of Strategy, Policy, and Plans

Samantha Vinograd /s/  
Senior Counselor for National Security  
Office of the Secretary

**SUBJECT: Organizing DHS Efforts to Counter Disinformation**

---

The spread of disinformation<sup>1</sup> presents serious homeland security risks:

- Conspiracy theories about the validity and security of elections may undermine trust in core democratic institutions, amplify threats against election personnel, and jeopardize the voting rights of vulnerable communities.
- Disinformation related to the origins and effects of COVID-19 vaccines or the efficacy of masks undercuts public health efforts to combat the pandemic.
- Foreign terrorists, nation-states, and domestic violent extremist (DVE) groups leverage disinformation narratives to amplify calls to violence, including racially or ethnically motivated and anti-government/anti-authority violence. These actors often amplify and exploit narratives that already exist in public discourse, such as disinformation surrounding the validity of the 2020 election underpinning calls to violence on January 6, 2021.
- Disinformation can complicate the performance of core DHS missions. Falsehoods surrounding U.S. Government immigration policy drive vulnerable populations to pay smugglers to bring them on the dangerous journey to our southern border. Disinformation can hamper emergency responders in the aftermath of natural disasters or other incident responses.

DHS efforts to combat disinformation must account for the sensitivities inherent to this mission:

- The Department must ensure its counter-disinformation efforts do not have the effect of chilling or suppressing free speech and free association or of infringing on individuals' privacy or other First Amendment protected activity.
- The protection of privacy, civil rights, and civil liberties must be incorporated into every step of this work and any overarching framework guiding its execution.

---

<sup>1</sup> The term disinformation will be used to reference any of mis-, dis-, or mal-information, or other terms of art that refer to false information that is intentionally or inadvertently injected into the information environment.

PRE-DECISIONAL/DELIBERATIVE

~~UNCLASSIFIED // FOR OFFICIAL USE ONLY~~



PRE-DECISIONAL/DELIBERATIVE  
~~UNCLASSIFIED // FOR OFFICIAL USE ONLY~~

**Subject: Organizing DHS Efforts to Counter Disinformation**  
**Page 2**

- The counter-disinformation mission, including the choices as to what issue areas to focus on, must not be politicized and must be protected from perceptions of politicization.
- DHS should not attempt to be an all-purpose arbiter of truth in the public arena. It should instead focus its efforts on disinformation impacting DHS core missions.
- DHS's role in responding to disinformation should be limited to areas where there are clear, objective facts (i.e., medical evidence regarding COVID; factual information about elections administration and security, DVE narratives) and where DHS has particular expertise and a strong oversight structure to ensure legal and policy review of any response efforts.
- DHS has a unique role to play in information sharing across the government, with SLTT entities, and with the public. DHS is uniquely situated to share information in an authoritative way, something that the private sector and academia cannot do. Conversely, information sharing carries risks for the Department and must be accomplished in a way that is perceived as unbiased and viewpoint neutral.
- In addition, the federal government may not always be the ideal or most trusted voice on a given topic. DHS should work closely as appropriate with state, local, tribal, and territorial (SLTT) authorities and private sector partners.

**DHS Functions and Existing Efforts to Counter Disinformation**

DHS components are already engaged in countering disinformation, with activities falling into five functions that are performed by the components themselves or through third-party resources: 1) identification of disinformation relevant to DHS's mission; 2) analysis of its source and influence; 3) information sharing regarding threats posed by disinformation, 4) response to the disinformation threat; and 5) building resilience to disinformation. There is also excellent work being done by interagency partners, the private sector, and academia—particularly concerning identifying and analyzing disinformation—and DHS should leverage this work when possible.

- 1) *Identification:* Information gathering on disinformation threats and trends.
  - I&A's Homeland Influence Task Force collects information on possible disinformation from publicly available sources as well as other intelligence sources where the collection furthers one of I&A's authorized intelligence missions, such as foreign intelligence and protection of critical infrastructure.
  - CISA gathered information on disinformation related to the elections with SLTT partners leading up to the 2020 election and has limited authority to collect information on disinformation related to critical infrastructure.
- 2) *Analysis:* Assessing the impact of specific disinformation narratives on the homeland or on DHS missions.
  - I&A, as well as other components engaging in intelligence and analytic functions, produce analysis on disinformation threats, whom they may be targeting, and what attendant risks might arise.
- 3) *Information Sharing:* Providing timely, quality information on disinformation threats and strategic trends to stakeholders including SLTT authorities, private sector partners, or the public directly.
  - Leading up to the 2020 election, CISA relayed reports of election disinformation from election officials to social media platform operators.

PRE-DECISIONAL/DELIBERATIVE  
~~UNCLASSIFIED // FOR OFFICIAL USE ONLY~~



PRE-DECISIONAL/DELIBERATIVE  
~~UNCLASSIFIED // FOR OFFICIAL USE ONLY~~

**Subject: Organizing DHS Efforts to Counter Disinformation**  
**Page 3**

- I&A distributes intelligence products to SLTT partners related to disinformation threats. Most recently, I&A issued a Public Safety Notification concerning the possible threat of violence motivated by conspiracy theories related to the “reinstatement” of former President Trump.
  - The August 13, 2021 National Terrorism Advisory System Bulletin referenced the threat of disinformation spread by foreign and domestic threat actors.
- 4) *Response:* Factually countering disinformation through public communications channels to mitigate related threats, increase awareness, and improve public safety.
- During the 2020 election, CISA maintained a ‘Rumor Control’ website to counter foreign disinformation related to the security and conduct of the vote. CISA sought to ‘prebunk’ incorrect claims with factual information.
  - In your August 12, 2021 public remarks in Brownsville, TX concerning the southwest border, you stated your intention to “debunk false information that has been spread,” sharing factual information about the situation on the ground and DHS’s border enforcement and policies.
- 5) *Building Resilience:* Improving the public’s ability to detect disinformation through digital and media literacy, where DHS has a unique role to play, programs and civic education. These programs are coordinated with federal, SLTT, and private sector partners.
- CISA launched a graphic novel series to reach potentially impacted communities in a non-traditional way. The novels educate on the dangers of disinformation and how to detect it.
  - PLCY is working with the Department of Education to build resilience to disinformation and CP3 Digital Forums and Community Awareness Briefings could further address digital media literacy, empowering communities to mitigate the harmful effects of content encouraging violence.
  - S&T Technology Centers are examining methods to mitigate disinformation, to include leveraging global research leaders on this topic and to provide scientific advice in support of Department initiatives.

**Models to Structure DHS Counter-Disinformation Efforts**

There are many possible ways to structure DHS counter-disinformation efforts moving forward. The models presented below for your consideration represent a spectrum of options, from fully federating counter-disinformation operations to operational components, to building in varying levels of Headquarters oversight, governance, and coordination.

**Option 1 Fully Federated Model: Operational Components Execute Independently**

The DHS counter-disinformation mission would be entirely federated to components, which would report to the Secretary and Deputy Secretary in the ordinary course but would not otherwise be governed by specific headquarters policies or guidance on this topic beyond existing DHS oversight functions. This model generally resembles the status quo in which components identify and prioritize disinformation threats in their respective mission spaces (sometimes relying on I&A intelligence reports), plan and execute operations, and conduct their own oversight and governance. It also means that each component operates under its own authorities, including the limits on these authorities.

**Option 2 Governance Board Model: Independent Component Execution Under an Overarching DHS Protective Framework**

Execution of DHS counter-disinformation operations would be federated to components, but subject to overarching Department-wide governance requirements to ensure that a common set of issue-agnostic safeguards and oversight tools are employed. PLCY could convene a governance board that would

PRE-DECISIONAL/DELIBERATIVE  
~~UNCLASSIFIED // FOR OFFICIAL USE ONLY~~



PRE-DECISIONAL/DELIBERATIVE

~~UNCLASSIFIED // FOR OFFICIAL USE ONLY~~

**Subject: Organizing DHS Efforts to Counter Disinformation**

**Page 4**

promulgate policy and legal requirements setting forth baseline requirements that all components must meet in their counter-disinformation work, to include protections ensuring compliance with applicable civil rights and civil liberties, privacy, and legal requirements, such as First Amendment and Privacy Act requirements. Members would include all components conducting counter-disinformation operations as well as CRCL, PRIV, OGC, I&A, S&T, and MGMT.

The board's role would not be prescriptive, instead providing components with guidelines and minimum safeguards applicable across disinformation missions, regardless of the topic. The board could also develop and share with components best practices, to include:

- Risk assessment methodologies to prioritize disinformation threats with a nexus to violence or that pose a direct risk to operations;
- Guidelines for partnering with or procuring counter-disinformation services from the private sector consistent with the sensitivities addressed above; and
- Best practices for auditing or other oversight of counter-disinformation operations.

The board could also convene DHS stakeholders when new disinformation threats emerge or are identified by interagency partners that do not clearly fit within a disinformation mission already being performed by a DHS component. The board would determine who within the Department is best positioned to address the threat, make recommendations to the Secretary as to how the new threat should be addressed, and support whichever operational component is taking on the mission in standing up with appropriate governance.

The board would not play a role in coordinating or overseeing operations. Components would determine the functions they need for their counter-disinformation missions and how they will perform them. For example, a component could conduct identification and analysis itself, or leverage reporting from I&A or another federal agency, or engage private sector services.

Components would also be responsible for partner engagement in their respective mission spaces, including with the interagency, SLTT authorities, private sector entities, tech platforms, and the general public. Components would work together as needed to coordinate engagement with partners to avoid organizations receiving overlapping outreach from multiple parts of the Department.

**Option 3 Disinformation Coordinator Model: Coordinated Oversight and Operations**

The most centralized approach could involve a newly-designated Coordinator for Countering Disinformation, modeled after the Department's Counterterrorism Coordinator. The Coordinator would work with components (and potentially non-DHS agencies should the administration encourage such an approach) to develop policies, procedures, and guidelines, and identify required resources to mature the Department's disinformation capabilities. Components would still be responsible for executing their respective disinformation missions, but the Coordinator would regularly convene components to facilitate the identification and analysis of disinformation threats and coordinate operational responses.

The Coordinator would also be responsible for developing homeland security counter-disinformation functions in coordination with components, other federal agencies, international partners, academia, non-profits, and the private sector, to include:

- Instituting Department-wide governance and oversight structures to ensure counter-disinformation efforts satisfy, among other considerations, civil rights and civil liberties, privacy, and legal (including First Amendment) requirements (similar to Option 2 above);

PRE-DECISIONAL/DELIBERATIVE

~~UNCLASSIFIED // FOR OFFICIAL USE ONLY~~

PRE-DECISIONAL/DELIBERATIVE  
~~UNCLASSIFIED // FOR OFFICIAL USE ONLY~~

**Subject: Organizing DHS Efforts to Counter Disinformation**

**Page 5**

- Growing DHS counter-disinformation capacity by ensuring components develop expertise through new hiring, training, and external partner engagement;
- Keeping apprised of the overall disinformation environment and coordinating action with relevant agencies and stakeholders on cross-cutting issues.
- Reviewing and making recommendations with respect to DHS authorities to counter disinformation;
- Developing policies for DHS public communications on disinformation as well as driving engagement with SLTT and private sector entities, including platform operators, together with components;
- Engaging SLTT authorities to respond to the disinformation threat, including through Fusion Centers and state homeland security advisors; and
- Serving as a central point of contact for interagency partners such as the White House, State's Global Engagement Center, DOJ, HHS, DOD, and the Intelligence Community.

\*\*\*\*\*

PLCY recommends Option 2, to ensure nimbleness and component ownership of their mission spaces, while also providing assurance that all programs across the Department will operate in a manner consistent with our values. All components recommend a fulsome discussion with you to chart the way forward in this challenging space, so that a detailed action and implementation plan can be developed based on your guidance.

PRE-DECISIONAL/DELIBERATIVE  
~~UNCLASSIFIED // FOR OFFICIAL USE ONLY~~



Release Authorized by Senator Grassley and Senator Hawley

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~  
PREDECISIONAL//DELIBERATIVE

U.S. Department of Homeland Security  
Washington, DC 20528



**Homeland  
Security**

January 31, 2022

**ACTION**

**MEMORANDUM FOR THE SECRETARY**

**FROM:** Robert Silvers  
Under Secretary  
Office of Strategy, Policy, and Plans

**ROBERT P  
SILVERS**

Digitally signed by  
ROBERT P SILVERS  
Date: 2022.02.01  
16:27:36 -05'00'

Jennifer Daskal  
Acting Principal Deputy General Counsel

**JENNIFER C  
DASKAL**

Digitally signed by  
JENNIFER C DASKAL  
Date: 2022.02.01  
17:58:32 -05'00'

**SUBJECT: Disinformation Governance Board Charter**

---

**Purpose:** To obtain your approval of the charter for the Disinformation Governance Board.

**Background:** On September 29, 2021, you directed headquarters and Component leadership to pursue a governance board model to coordinate efforts to counter mis-, dis-, and mal-information (MDM) across the Department.<sup>1</sup> You emphasized the need for clarity as to the Department's policies, standards, and best practices related to MDM work. You also concluded that operational efforts to counter MDM should largely be carried out by Components, which would be responsible for their respective mission areas subject to the oversight of the governance board.

Based on that guidance, we developed the attached charter for a DHS Disinformation Governance Board ("the Board") to execute this critical work. The Board will ensure Departmental efforts to counter MDM are coordinated, deconflicted, and harmonized. The Board's primary roles are to develop and support the implementation of best practices, policies, and protocols that support the identification, assessment, response, and resilience to MDM threats, and that do so in a way that ensures respect for privacy, civil rights, and civil liberties. The Board will also support and coordinate, in conjunction with the relevant Components, MDM work with other departments and agencies, the private sector, and non-governmental actors. In addition, the Board will support research and development efforts to understand the MDM threat to homeland security.

The Board will be co-chaired by representatives of the Office of Strategy, Policy, and Plans (PLCY) and the Office of the General Counsel. Members will include components engaged in

---

<sup>1</sup> This model is presented as Option 2 in the September 13, 2021 memorandum 'Organizing DHS Efforts to Counter Disinformation.'

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~  
PREDECISIONAL//DELIBERATIVE

Release Authorized by Senator Grassley and Senator Hawley

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~  
PREDECISIONAL//DELIBERATIVE

**Subject: Disinformation Governance Board Charter**  
**Page 2**

counter-MDM activities or that provide oversight and support for such activities. Members will be represented by the principal or deputy for their respective Component/Offices.

The Board will meet no less than once per quarter for the first two years of its existence. It will be supported by a Steering Group, consisting of representatives designated by each Member. A senior official from within PLCY will serve as Executive Director for the Board and Chair of the Steering Group, to be supported by an Executive Secretariat comprised of staff detailed or assigned to PLCY. As we build, we may enlist your office's support in obtaining detailees or other staffing.

The Charter has been coordinated with all DHS components that will be Members of the Board.

For your awareness, we attach a copy of the MDM Playbook that PLCY, together with components, developed for countering MDM in a unified way across the Department in the context of the current situation in Ukraine. We are enthusiastic about the further work that the Disinformation Governance Board can accomplish.

**Timeliness:** We request your signature of the charter as soon as practicable.

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~  
PREDECISIONAL//DELIBERATIVE

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

**Subject: Disinformation Governance Board Charter**  
**Page 3**

**Recommendation:** Approve the charter for the Disinformation Governance Board.

Approve/date

  
2/24/22

Disapprove/date

Modify/date

Needs discussion/date

**Attachments:**

- A. Disinformation Governance Board Charter
- B. Ukraine MDM Playbook
- C. 'Organizing DHS Efforts to Counter Disinformation' (September 13, 2021)

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~



~~FOR OFFICIAL USE ONLY~~ / DELIBERATIVE / DRAFT

## **DHS Disinformation Governance Board**

### **Charter**

#### **Section 1. Purpose**

The DHS Disinformation Governance Board ("Board") will guide and support the Department's efforts to address mis-, dis-, and mal-information that threatens homeland security ("MDM"). Whereas Department Components will lead on operational responses to MDM in their relevant mission spaces, the Board will ensure DHS efforts are coordinated, deconflicted, and harmonized, both within DHS and across the interagency, to ensure efficiency, unity of effort, and promotion of applicable compliance and best practices.

The Board will focus on the following four cross-functional lines of effort to counter MDM, many of which are already underway ("lines of effort"): (1) identifying MDM ("Identification"); (2) assessing and analyzing the risk that such MDM poses to homeland security ("Risk Assessment"); (3) responding to these MDM threats ("Response"); and (4) building resilience to MDM ("Building Resilience").

With respect to each of these lines of effort, the Board will develop and support the implementation of governance policies and protocols that, among other issues, protect privacy, civil rights, and civil liberties; harmonize and support coordination with other departments and agencies, the private sector, and non-governmental organizations; and support research and development efforts to assess and combat MDM.

#### **Section 2. Members**

The Board will be co-chaired by representatives of the Office for Strategy, Policy, and Plans (PLCY) and the Office of the General Counsel (OGC). Standing Board members will be representatives of the following DHS Components: the Management Directorate (MGMT); Office of Intelligence and Analysis (I&A); Science and Technology Directorate (S&T); Privacy Office (PRIV); Office for Civil Rights and Civil Liberties (CRCL); Office of Public Affairs (OPA); Cybersecurity and Infrastructure Security Agency (CISA); Federal Emergency Management Agency (FEMA); and U.S. Customs and Border Protection (CBP). Representatives shall be the Principal or Deputy for their respective Component. Other Components may be invited to either join the Board or participate on an ad hoc basis, as appropriate and needed.

#### **Section 3. Structure**

The Board will be supported by a Steering Group, which will consist of a representative from each Component participating in the Board. Each representative will be selected by their respective Board member.

~~FOR OFFICIAL USE ONLY~~ / DELIBERATIVE / DRAFT

The Board co-chairs will designate a DHS senior official to serve as the Executive Director for the Board and Chair of the Steering Group. The Executive Director will be detailed or assigned to PLCY, where they will be supported by an Executive Secretariat for the Board comprising staff detailed or assigned to PLCY. The Executive Director will attend and may participate in all Board meetings.

#### **Section 4. Board Responsibilities**

Components will lead on MDM-related operational responses and other efforts to counter MDM in their relevant mission spaces. The Board will serve as the central forum in the Department to ensure consistent governance and coordination of such efforts, and adherence to applicable constitutional, statutory, and regulatory authorities and obligations.

The Board's initial responsibilities will include a review of existing MDM governance policies and practices across the Department, including:

- policies, procedures, practices, plans, and standards to ensure compliance with applicable constitutional, statutory, and regulatory obligations;
- policies, procedures, practices, plans, and standards to ensure appropriate privacy and civil rights and civil liberties protections;
- policies, procedures, practices, plans, and standards for interactions with the private, non-profit, and academic sectors; and,
- relevant procurement policies and practices.

Based, in part, on the findings from its initial review, the Board will be responsible for developing MDM-related guidance, best practices, and recommendations regarding:

- compliance with applicable constitutional, statutory, and regulatory obligations;
- standards for and implementation of appropriate privacy, civil rights, and civil liberties protections;
- procurement guidelines for contracting or funding third parties to support the Department's MDM efforts;
- grant funding and cooperative agreements;
- development and implementation of new technological and data management tools; and,
- any other applicable guidance, best practices, and recommendations to guide the aforementioned four lines of effort.

The Board also will coordinate, deconflict, and harmonize departmental efforts to address MDM, including by:

- receiving regular and routine updates from DHS Components, the Intelligence Community, and other interagency partners on MDM;
- harmonizing and deconflicting activities by DHS Components regarding the lines of effort;
- harmonizing, deconflicting, and coordinating, in conjunction with relevant Components, the Department's external engagement regarding MDM;



~~FOR OFFICIAL USE ONLY~~ / DELIBERATIVE / DRAFT

- serving as the Department's internal and external point of contact for coordination with state, local, tribal, and territorial partners, the private sector, and non-governmental actors regarding MDM; and,
- serving as the Department's internal and external point of contact for receiving, coordinating, responding to, and interacting with interagency partners, including the Executive Office of the President, for policy matters generally related to mis-, dis-, and mal-information, but not related to the performance of intelligence activities.

## **Section 5. Roles and Responsibilities of Board Members**

The co-chairs of the Board will:

- convene the Board as needed;
- approve the agenda for Board meetings;
- preside over Board meetings;
- approve summaries of conclusions reached during the Board meetings;
- communicate Board decisions and activities to the Secretary and other DHS leadership, as appropriate;
- represent the Board to external audiences; and,
- take all other actions necessary and proper for the execution of the Board's responsibilities.
- 

The Board Members will:

- represent the perspectives of their respective Components at Board meetings;
- review any proposals submitted to the Board; and,
- ensure that their respective Components implement, execute, and follow Board decisions.

The Executive Director will:

- propose agenda items and discussion topics for the Board following Steering Group review;
- communicate the positions taken at the Steering Group concerning proposals before the Board;
- propose summaries of conclusion for each Board and Steering Group meeting;
- implement and execute Board decisions through the Steering Group;
- supervise the activities of the Executive Secretariat; and,
- represent the Steering Group and, where appropriate and in coordination with the co-chairs, the Department to external audiences on MDM-related matters.

The Steering Group Members will:

- represent the perspectives of their respective Components at Steering Group meetings;
- review and discuss any proposals to be submitted to the Board;
- communicate their considerations of Board proposals to their respective Board Members, the Executive Director, and other members of the Steering Group;

~~FOR OFFICIAL USE ONLY~~ / DELIBERATIVE / DRAFT

- review and approve summaries of conclusions of Steering Group meetings; and,
- subject to the direction and guidance of their respective Board Members, help ensure that their respective Components implement, execute, and follow Board decisions.

#### **Section 6. Processes & Procedures**

The Board will meet regularly at the discretion of the co-chairs and no less than once per quarter for the first two years of the Board's existence. The Steering Group will meet at the discretion of the Board or Executive Director. Issues raised and proposals submitted to the Board will be resolved by consensus to the greatest extent possible. Where there is a disagreement amongst the Board members, the Board will resolve the matter before it by majority vote. In the absence of consensus, any Board member may elevate, in the form of a written memorandum, an issue to the Secretary or Deputy Secretary where they believe that a decision made by the Board implicates their statutory or other assigned authorities.

The Steering Group is not a voting body. Instead, its members will discuss all issues brought before it and make their recommendations to the Board. Steering Group members will support the development of consensus recommendations to the Board to the greatest extent possible.

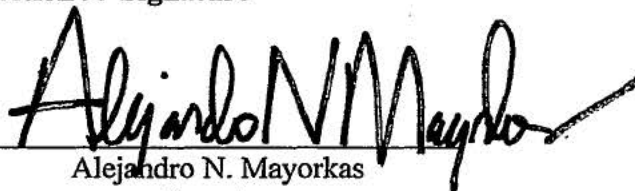
#### **Section 7. Relationship to Other Departmental Governance Bodies**

The Board will serve as the departmental forum for governance of DHS policies, plans, procedures, standards, and activities pertaining to MDM that threatens homeland security. As such, all DHS-wide or Component-specific proposals for funding related to efforts to counter MDM should be appropriately coordinated with the Board, including in advance of submitting any final funding proposals. Matters raised before the Board may implicate other departmental governance fora already in existence. Where that occurs, the Board will coordinate its activities with those respective fora through the Executive Director.

#### **Section 8. Effective Date**

This charter will go into effect when signed by the Secretary of Homeland Security.

#### **Section 9. Signature**

  
Alejandro N. Mayorkas  
Secretary

U.S. Department of Homeland Security

Feb. 24, 2022  
Date



~~FOR OFFICIAL USE ONLY~~

## Twitter

April 28, 2022 (TBC)

### Overview:

- You will meet in person with Twitter executives Nick Pickles, Head of Policy, and Yoel Roth, Head of Site Integrity, for XX minutes on public-private partnerships, MDM, and countering DVE. The meeting is off the record and closed press.
  - You have previously met with Jessica Herrera-Flanigan, Twitter's Vice President of Public Policy and Philanthropy for the Americas.
  - Please note any other main external participants who will be joining the principal (i.e. co-speakers on a panel).
  - You will be staffed by [REDACTED]

Commented [KE1]: Placeholder.

### Key Objectives:

- This meeting is an opportunity to discuss operationalizing public-private partnerships between DHS and Twitter, as well as inform Twitter executives about DHS work on MDM, including the creation of the Disinformation Governance Board and its analytic exchange, and the Department's ongoing DVE work.

### Flow of Show:

- 1:45 pm ET: [Example] Tech check prior to meeting.
- 2:30 pm ET: Event concludes.

Commented [KE2]: Placeholder.

### Background:

- Note:** Nick and Yoel both know DGB Executive Director Nina Jankowicz.
- Propose** that Twitter become involved in Disinformation Governance Board Analytic Exchanges on Domestic Violent Extremism (DVE) and Irregular Migration.
  - Thank** Twitter for its continued participation in the CISA Analytic Exchange on Election Security.
- Ask** what types of data or information would be useful for Twitter to receive in Analytic Exchanges or other ways the Department could be helpful to Twitter's counter-MDM efforts.

Commented [KE3]: All: Please include any info on recent engagements with Twitter.

### Participants:

U/S Silvers

[REDACTED] Managing Director for Strategy

### External:

(Principal), (Role)

(Staffer), (Role)

(Staffer), (Role)

[PAGE BREAK BEFORE DISCUSSION POINTS]

~~FOR OFFICIAL USE ONLY~~



~~FOR OFFICIAL USE ONLY~~

~~FOR OFFICIAL USE ONLY~~

~~FOR OFFICIAL USE ONLY~~

#### Discussion Points:

##### DHS Efforts on MDM

- **Introduce** the Disinformation Governance Board.
  - The Board will ensure that DHS is actively and efficiently leveraging all its available resources and capabilities to mitigate and counter disinformation with a homeland security nexus, consistent with a deep commitment to protecting privacy and free speech.
  - The Board will serve as a coordinating mechanism for the Department's outreach to industry, civil society, and international partners on MDM.
- The Board's initial work plan includes establishing analytic exchanges with industry on countering MDM related to domestic violent extremism and irregular migration.
  - **Propose** that Twitter be an active participant in these exchanges and thank the company for their continued engagement with CISA's election security exchange.

##### Operationalizing Public/Private Partnerships

Commented [KE4]: CISA and CP3 please add TPs

##### DVE

- The United States remains deeply concerned regarding the complex, cross-cutting links between MDM and all forms of violent extremism.
- The primary terrorism-related threat to the United States continues to stem from lone offenders or small cells of individuals who are motivated by a range of foreign and/or domestic grievances often cultivated through the consumption of certain online content.
- Key factors contributing to the current heightened threat environment include:
  - The proliferation of false or misleading narratives, which sow discord or undermine public trust in U.S. government institutions.
  - Continued calls for violence directed at U.S. critical infrastructure; soft targets and mass gatherings; faith-based institutions, such as churches, synagogues, and mosques; institutions of higher education; racial and religious minorities; government facilities and personnel, including law enforcement and the military; the media; and perceived ideological opponents.
  - Calls by foreign terrorist organizations for attacks on the United States based on recent events.
- In June, the White House released the first ever *National Strategy for Combatting Domestic Terrorism*. In response, DHS has realigned and dedicated resources to combat domestic violent extremists (DVEs) and would like to have a deeper discussion on our latest assessments.
  - The DHS Office of Intelligence and Analysis (or I&A) created a domestic terrorism branch within its counterterrorism mission center to ensure DHS develops the expertise necessary to produce sound and timely intelligence, at the lowest classification possible in order to inform our stakeholders.
  - The Department established a new Center for Prevention Programs and Partnerships (CP3) to improve the Department's ability to combat terrorism and targeted

3

~~FOR OFFICIAL USE ONLY~~

~~FOR OFFICIAL USE ONLY~~

violence, consistent with privacy protections, civil rights and civil liberties, and other applicable laws.

- We are working to improve our ability to identify narratives that are playing out online in effort to counter the threat that is increasingly manifesting through various digital forums

#### Ukraine

- Together with partners from across the U.S. Government, DHS components – including CISA, FEMA, TSA, the U.S. Coast Guard, and our policy and legal staffs are preparing for a range of potential scenarios.
  - Our goal is to ensure that – well in advance of any potential incident – we are connecting operators from across our government and the private and civil sectors so we can identify and work to remediate an emerging campaign as quickly as possible.
  - Twitter participated in a CISA/FBI led call with social media companies on February 25<sup>th</sup> to discuss potential of influence operations stemming from the escalating geopolitical issues as it relates to U.S. critical infrastructure.
- Following actions taken by the U.S. and allies, we have seen increased instances of MDM and malign foreign influence on publicly available websites that may be linked to the Russian government, military, and intelligence services in the Russian and Ukrainian languages. These include allegations that the United States is deploying military forces to Ukraine's eastern front and that U.S. intelligence services are staging false-flag attacks in Ukraine to instigate a conflict.

#### **Hard Q&A:**

- What questions do we expect and/or know will come up in this meeting?
  - Please provide a concise recommended response.

#### **Attachments**

##### **A. Biographies**

---

**Staff Responsible for Briefing Memo: Nina Jankowicz, Executive Director DHS  
Disinformation Governance Board, [REDACTED]**

~~FOR OFFICIAL USE ONLY~~



~~FOR OFFICIAL USE ONLY/ DELIBERATIVE~~**DHS Disinformation Governance Board Charter**

**Section 1. Purpose.** The purpose of the Board is to support the Department's efforts to address mis-, dis-, and mal-information (MDM) that threatens homeland security. Departmental components will lead on operational responses to MDM in their relevant mission spaces. The Board will ensure these activities are conducted within a protective governance framework that respects privacy, civil rights, and civil liberties. This work will be speaker-agnostic, focusing on the narratives rather than those who originate or spread them. The board will also ensure that Departmental efforts are coordinated and deconflicted to ensure efficiency, unity of effort, and promotion of best practices across the Department's MDM work.

More specifically, the Board's primary roles are three-fold: 1) To develop and implement governance policies for departmental efforts related to MDM, 2) To deconflict departmental efforts to counter MDM narratives that threaten homeland security, including with respect to departmental engagement with third parties; and 3) To streamline and enhance coordination with other departments and agencies and promote best practices for counter-MDM work.

These efforts will focus on four lines of effort (LOEs) that cut across efforts to counter MDM across DHS's many mission spaces: (1) identifying narratives of concern ("Identification"); (2) assessing and analyzing the risk that such narratives pose to homeland security ("Risk Assessment"); (3) responding to these narratives ("Response"); and (4) developing resilience against MDM ("Building Resilience").

**Sec. 2. Members.** The Board will be co-chaired by the Office for Strategy, Policy, and Plans (PLCY) and the Office of the General Counsel (OGC). Standing Board members will be the following: the Management Directorate; the Office of Intelligence and Analysis (I&A); the Science and Technology Directorate (S&T); the Privacy Office (PRIV); the Office for Civil Rights and Civil Liberties (CRCL); the Office of Public Affairs (OPA); the Cybersecurity and Infrastructure Security Agency (CISA); the Federal Emergency Management Agency (FEMA); and U.S. Customs and Border Protection (CBP). Other components may be invited to participate on an ad hoc basis.

**Sec. 3. Structure.**

Each Board member will be represented by the Principal or Deputy for their respective component. The Board will be supported by a DHS MDM Steering Group, which will consist of representatives for each component participating in the Board selected by their respective Board member. In addition, the Secretary will designate a senior official from within the Department to serve as the Executive Agent for the Board and Chair of the Steering Group. The Executive Agent will be detailed or assigned to PLCY, where they will be supported by an Executive Secretariat for the Board and Steering Group comprising staff detailed or assigned to PLCY. The Executive Agent will attend and may participate in all Board meetings.

**Sec. 4. Roles & Responsibilities.**

Department components will lead on operational responses to MDM in their relevant mission space. The Board will serve as the central forum in the Department to ensure consistent governance and coordination of such efforts.

- The Board's initial responsibilities will include a review of existing MDM governance policies and practices across the Department, including—
  - Policies, procedures, practices, plans, and standards to ensure compliance with applicable constitutional, statutory, and regulatory obligations;

~~FOR OFFICIAL USE ONLY~~ DELIBERATIVE

- Policies, procedures, practices, plans, and standards to ensure appropriate privacy and civil rights and civil liberties protections;
- Policies, procedures, practices, plans, and standards for interactions with the private, non-profit, and academic sectors; and
- Relevant procurement policies and practices.
- The Board will also be responsible for developing guidance, best practices, and recommendations with respect to—
  - Compliance with applicable constitutional, statutory, and regulatory obligations;
  - Ensuring the implementation of appropriate privacy and civil rights and civil liberties protections;
  - Proposals for additional or amended departmental authorities or funding, consistent with the processes of the Deputies Management Action Group (DMAG);
  - Procurement guidelines for contracting with third parties to support the Department's MDM efforts;
  - Grant funding; and
  - Any other applicable best practices to guide the lines of effort with respect to identification, risk assessment, response, and building resilience.

The Board also will coordinate and deconflict departmental efforts to address MDM narratives that threaten homeland security. This will include—

- Receiving regular and routine updates from Departmental components on MDM narratives of concern and the relevant MDM lines of effort;
- Deconflicting any activities by the Department and relevant components to counter MDM with respect to external outreach to the private and other nongovernmental actors;
- Serving as a departmental point of contact, in addition to component points of contact, as appropriate, for receiving and assessing concerns about MDM raised by federal, state, local, tribal, private sector, or other nongovernmental partners; and
- Serving as a departmental point of contact, in addition to component points of contact, for receiving, coordinating, responding to, and interacting with interagency partners, including the Executive Office of the President, for all MDM matters not related to the performance of intelligence activities.

The Co-Chairs of the Board will—

- Convene the Board;
- Compose the agenda for Board meetings;
- Preside over Board meetings;
- Approve and disseminate summaries of conclusions reached at the Board meetings;
- Communicate Board decisions and activities as they deem appropriate to the Secretary and Deputy Secretary;
- Represent the Board to external audiences; and
- Take all other actions necessary and proper to execution of the Board's responsibilities.

The Board members will—

- Represent the perspectives of their respective offices or components at Board meetings;
- Review and either approve or reject any proposals submitted to the Board; and
- Ensure that their respective components implement, execute, and follow Board decisions.



~~FOR OFFICIAL USE ONLY~~ DELIBERATIVE

The Executive Agent will—

- Propose agenda items and discussion topics for the Board following Steering Group review;
- Communicate the position(s) taken at the Steering Group concerning proposals before the Board;
- Propose summaries of conclusion for each Board meeting;
- Implement and execute Board decisions through the Steering Group;
- Supervise the activities of the Executive Secretariat; and
- Represent the Steering Group and, where appropriate and in coordination with the Co-Chairs, the Department to external audiences on matters concerning MDM.

The Steering Group members will—

- Represent the perspectives of their respective offices or components at Steering Group meetings;
- Review and either endorse or oppose any proposals to be submitted to the Board;
- Communicate their endorsements or oppositions to Board proposals to their respective Board members, the Executive Agent, and other members of the Steering Group; and
- Subject to the direction and guidance of their respective Board members, help to ensure that their respective components implement, execute, and follow Board decisions.

**Sec. 5. Processes & Procedures.**

The Board will meet regularly and at the discretion of the Co-Chairs, but in any event no less than once per quarter for the first two years of the Board's existence. The Steering Group will meet at the discretion of the Executive Agent. Issues raised and proposals submitted to the Board will be resolved by consensus to the greatest extent possible. Where there is a disagreement amongst the Board members, the Board will resolve the matter before it by majority vote. In the absence of consensus, any Board member may elevate, in a form of a written memorandum, an issue to the Secretary or Deputy Secretary where they believe that a decision made by the Board implicates their statutory or other assigned responsibilities.

The Steering Group is not a voting body. Instead, its members will make recommendations to the Board, as communicated by the Executive Agent. The Steering Group members will endeavor to make consensus recommendations to the Board to the greatest extent possible. The Executive Agent will prepare draft summaries of conclusion after each Board meeting. The Co-Chairs will review and approve the summaries of conclusion before they are socialized with the other Board members.

**Sec. 6. Relationship to Other Departmental Governance Bodies.**

The Board will serve as the senior departmental forum for governance of departmental policies, plans, procedures, standards, and activities pertaining to MDM. As such, all proposals for funding through the DMAG concerning efforts to counter MDM must be coordinated in advance with the Board. Matters raised before the board may implicate other departmental governance fora already in existence. Where that occurs, the Board will coordinate its activities with those respective fora through the Executive Agent.

**Sec. 7. Effective Date.**

The charter will go into effect when signed by the Secretary of Homeland Security.

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~  
PREDECISIONAL//DELIBERATIVE

U.S. Department of Homeland Security  
Washington, DC 20528



**Homeland  
Security**

## ACTION

### MEMORANDUM FOR THE SECRETARY

**FROM:** Robert Silvers  
Under Secretary  
Office of Strategy, Policy, and Plans

Jonathan Meyer  
General Counsel

**SUBJECT:** DHS Disinformation Governance Board Charter

---

**Purpose:** To obtain your approval of the charter for the DHS Disinformation Governance Board.

**Background:** In a September 29, 2021 discussion with headquarters and Component leadership, you directed the Department to pursue a governance board model to coordinate efforts to counter mis-, dis-, and mal-information (MDM).<sup>1</sup> You discussed the benefits of having a mechanism that would develop and coordinate intra-Departmental governance policies, standards, and best practices related to MDM work and that could coordinate efforts to engage private sector stakeholders. Execution of DHS counter-MDM activities would be federated to Components, who would be responsible for their respective mission areas subject to the oversight of the governance board.

Based on your guidance, we have developed the attached charter for a DHS Disinformation Governance Board (Board) to execute this critical work. The Board's primary roles would be three-fold: 1) To develop and implement governance policies for departmental efforts related to MDM; 2) To deconflict, where necessary, departmental efforts to counter MDM narratives that threaten homeland security, including with respect to departmental outreach engagement with third parties; and 3) To streamline and enhance coordination with other departments and agencies and promote best practices for counter-MDM work.

The Board will be co-chaired by the Office of Strategy, Policy, and Plans (PLCY) and the Office of the General Counsel. Members will include all Components and headquarters offices engaged in counter-MDM activities or providing oversight and support for such activities. The Board's guidance will include protections that ensure compliance with applicable law and policy and

---

<sup>1</sup> This model is presented as Option 2 in the September 13, 2021 memorandum 'Organizing DHS Efforts to Counter Disinformation.'



~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~  
PREDECISIONAL//DELIBERATIVE

**Subject: DHS Disinformation Governance Board Charter**  
**Page 2**

protect individuals' privacy, civil rights, and civil liberties. Members will be represented by the principal or deputy for their respective Component/Offices.

The Board will meet no less than once per quarter for the first two years of its existence. It will be supported by a Steering Group, consisting of representatives designated by each member. You will designate a senior official from within the Department to serve as Executive Agent for the Board and Chair of the Steering Group, who would be supported by an Executive Secretariat comprising staff detailed or assigned to PLCY.

Chartering the Board would provide structure and oversight to critical efforts already underway, including: 1) a review of existing policies and practices to protect privacy, civil rights, and civil liberties; 2) developing a framework for the Department to notify specific entities, or in some cases the public, of MDM relevant to homeland security; and 3) reviewing opportunities for deeper information sharing and exchange of best practices with platform operators and other private sector partners.

**Timeliness:** MDM constitutes a significant and immediate threat to homeland security. We request your signature of the charter by January 31 to allow for the first meeting of the Board to occur by the end of February.

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~  
PREDECISIONAL//DELIBERATIVE



**Subject: DHS Disinformation Governance Board Charter**

**Page 3**

**Recommendation:** Approve the charter for the DHS Disinformation Governance Board.

Approve/date \_\_\_\_\_ Disapprove/date \_\_\_\_\_

Modify/date \_\_\_\_\_ Needs discussion/date \_\_\_\_\_

**Attachments:**

- A. Disinformation Governance Board Charter
- B. 'Organizing DHS Efforts to Counter Disinformation' (September 13, 2021)

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~  
**PREDECISIONAL//DELIBERATIVE**

Release Authorized by Senator Grassley and Senator Hawley

JOSH HAWLEY  
MISSOURI  
115 RUSSELL SENATE OFFICE BUILDING  
TELEPHONE: (202) 224-6154  
FAX: (202) 228-0526  
WWW.HAWLEY.SENATE.GOV

## United States Senate

WASHINGTON, DC 20510-2509

COMMITTEES  
JUDICIARY  
ARMED SERVICES  
HOMELAND SECURITY  
AND GOVERNMENTAL AFFAIRS  
SMALL BUSINESS  
AND ENTREPRENEURSHIP

April 28, 2022

The Honorable Alejandro Mayorkas  
Secretary of Homeland Security  
U.S. Department of Homeland Security  
245 Murray Lane, S.W.  
Washington D.C. 20528

**RECEIVED**  
By ESEC at 9:22 am, Apr 28, 2022

Dear Secretary Mayorkas:

I write with deep concern about the Department of Homeland Security's decision to create a new Disinformation Governance Board. I confess, I at first thought this announcement was satire. Surely no American Administration would ever use the power of Government to sit in judgment on the First Amendment speech of its own citizens. Sadly, I was mistaken. Rather than protecting our border or the American homeland, you have chosen to make policing Americans' speech your priority. This new board is almost certainly unconstitutional and should be dissolved immediately.

For well over a year, your Department has consistently treated competing policy views as disinformation to be monitored or investigated. However, political debates on issues such as immigration, pandemic lockdowns, and foreign policy clearly constitute "core political speech" protected by the First Amendment.<sup>1</sup> The Supreme Court has even gone so far as to say that "Under the First Amendment there is no such thing as a false idea."<sup>2</sup> The apparent broad mandate of this new government entity to "coordinate countering misinformation" in America undermines the argument that it can even exist consistent with the Constitution.<sup>3</sup>

Particularly troubling is your choice to lead the new board, Nina Jankowicz, a supposed "expert" with a long history of partisan attacks. Consider:

- In 2020, she described President Trump's use of the national guard as "a sentence I expect to hear from leaders of authoritarian countries, not the President of the United States."<sup>4</sup>
- In 2021, she quoted with praise an article that said "homegrown fascism predated President Donald Trump."<sup>5</sup>
- She has said America is systemically racist.<sup>6</sup>
- In response to revelations about Hunter Biden's laptop, she tweeted that "50 former natsec officials and 5 former CIA heads that believe the laptop is a Russian influence op. Trump says 'Russia, Russia, Russia.'"<sup>7</sup>

<sup>1</sup> *Meyer v. Grant*, 486 U.S. 414, 422 (1988).

<sup>2</sup> *Gertz v. Robert Welch, Inc.*, 418 U.S. 323, 339 (1974).

<sup>3</sup> <https://www.politico.com/newsletters/playbook/2022/04/27/fauci-pulls-out-of-whcd-is-biden-next-00028131>

<sup>4</sup> <https://twitter.com/wiczipedia/status/1267589264440729600>

<sup>5</sup> <https://twitter.com/wiczipedia/status/1321123630403694593>

<sup>6</sup> <https://twitter.com/wiczipedia/status/1311123042387529734>

<sup>7</sup> <https://twitter.com/wiczipedia/status/1319463138107031553?s=20&t=EZYZWppGDhzWKHE5ensHnQ>



Jankowicz has said the new DHS Board will “maintain the Dept’s commitment [sic] to protecting free speech.”<sup>8</sup> This is particularly ironic given Jankowicz’s extensive criticism of free speech and the First Amendment. Jankowicz has claimed that “the ‘free speech vs censorship’ framing is a false dichotomy.”<sup>9</sup> And when Elon Musk announced his acquisition of Twitter, she said “I shudder to think about if free speech absolutists were taking over more platforms, what that would look like for the marginalized communities ... which are already shouldering ... disproportionate amounts of this abuse.”<sup>10</sup> Jankowicz has even described opponents of social media speech codes as “first amendment zealots.”<sup>11</sup> These statements that question the value of free speech are obviously disqualifying for such a role.

While Democrats have for years controlled the public square through their Big Tech allies, Mr. Musk’s acquisition of Twitter has shown just how tenuous that control is. It can only be assumed that the sole purpose of this new Disinformation Governance Board will be to marshal the power of the federal government to censor conservative and dissenting speech. This is dangerous and un-American. The board should be immediately dissolved.

So that Congress can consider remedial legislation, please provide the following responses prior to your expected testimony before the Senate Homeland Security and Governmental Affairs Committee on May 4, 2022:

1. How will this Disinformation Board function? And who exactly will it be monitoring?
2. What analysis did DHS conduct, if any, to ensure that the Disinformation Board and its activities comport with the First Amendment?
3. Why did DHS time its announcement of this governance board directly after Mr. Musk’s acquisition of Twitter?
4. Who appointed Ms. Jankowicz to head the board as executive director? Were you aware of her history of partisan conduct prior to her appointment?
5. Has DHS conferred with any private social media company in the creation or operation of this board?

Sincerely,



Josh Hawley  
United States Senator

<sup>8</sup> <https://twitter.com/wiczipedia/status/1519282822158110721>

<sup>9</sup> <https://twitter.com/JackPosobiec/status/1519397817260904454?s=20&t=ukuMjyeX1tNluHKa1DmtGw>

<sup>10</sup> <https://www.npr.org/2022/04/16/1093212502/women-face-disproportionate-attacks-online-one-expert-shares-some-of-the-details>

<sup>11</sup> <https://twitter.com/wiczipedia/status/1192897252328714240>

**Department of Homeland Security Response to  
Senator Hawley's April 27, 2022 Letter**

**1. How will this Disinformation Board function? And who exactly will it be monitoring?**

For nearly 10 years, different agencies across DHS have worked to address disinformation that threatens our homeland security. The Department is deeply committed to doing all of its work in a way that protects Americans' freedom of speech, civil rights, civil liberties, and privacy. In fact, the Disinformation Governance Board is an internal working group that was established with the explicit goal of ensuring these protections are appropriately incorporated across DHS's disinformation-related work and that rigorous safeguards of Americans' fundamental rights are in place. The working group also seeks to coordinate the Department's engagements on this subject with other federal agencies and a diverse range of external stakeholders. The working group does not have any operational authority or capability.

The Department is focused on disinformation that threatens the security of the American people, including disinformation spread by foreign states such as Russia, China, and Iran, or other adversaries such as transnational criminal organizations and human smuggling organizations. Such malicious actors often spread disinformation to exploit vulnerable individuals and the American public, including during national emergencies.

DHS would be failing in its mission if it ignored disinformation that poses a threat to the homeland. To that end, Components seek to address disinformation related to their authorized missions. Some examples of that are as follows:

- U.S. Customs and Border Protection (CBP) counters disinformation that cartels and human smugglers spread to migrants to persuade them to cross our southwest border illegally. CBP's work includes its "Say No to the Coyote" campaign, making clear that entering the United States illegally is a crime.
- In 2012, during Hurricane Sandy, the Federal Emergency Management Agency (FEMA) corrected false information about the safety of drinking water and the location of shelters to protect and serve the hurricane's victims. FEMA has since built capacity to identify and respond to false information during major disaster responses, including Hurricanes Maria and Ida, during which FEMA provided critical information to protect disaster survivors from targeted scams. FEMA also ensures that disinformation campaigns do not prevent Americans from accessing federal aid during and after disasters.
- The Cybersecurity and Infrastructure Security Agency (CISA) works with private sector stakeholders to mitigate the risk of disinformation to U.S. critical infrastructure, work that has continued in light of Russia's invasion of Ukraine.

The working group is co-chaired by the DHS Office of Strategy, Policy, and Plans and Office of the General Counsel, and includes other DHS leaders from CISA, FEMA, CBP, the Office for Civil Rights and Civil Liberties, Office of Intelligence and Analysis, Science and Technology Directorate, and Privacy Office.

**2. What analysis did DHS conduct, if any, to ensure that the Disinformation Board and its activities comport with the First Amendment?**

The Department is deeply committed to doing all of its work in a way that protects Americans' freedom of speech, civil rights, civil liberties, and privacy. In fact, the Disinformation

**Department of Homeland Security Response to  
Senator Hawley's April 27, 2022 Letter**

Governance Board is an internal working group that was established with the explicit goal of ensuring these protections are appropriately incorporated across DHS's disinformation-related work and that rigorous safeguards of Americans' fundamental rights are in place.

It is co-chaired by the DHS Office of Strategy, Policy, and Plans and the Office of the General Counsel, and its membership includes departmental leaders from other DHS components, including those from the Office for Civil Rights and Civil Liberties and the Office of Privacy. The Office for Civil Rights and Civil Liberties and Privacy Officer were consulted prior to the establishment of the Board and through the development and publication of its charter.

Secretary Mayorkas will request that the bipartisan Homeland Security Advisory Council (HSAC) make recommendations for how the Department can most effectively and appropriately address disinformation that poses a threat to the homeland, while protecting free speech and other fundamental rights, and that HSAC Co-Chair Jamie Gorelick and HSAC Member Michael Chertoff lead this effort. Ms. Gorelick is a former U.S. Deputy Attorney General and Mr. Chertoff was Secretary of Homeland Security during President George W. Bush's Administration. At Secretary Mayorkas's request, DHS is exploring additional ways to enhance the public's trust in this important work.

**3. Why did DHS time its announcement of this governance board directly after Mr. Musk's acquisition of Twitter?**

The timing of the announcement was not related to any such external events. The Board's Charter was signed in February 2022.

**4. Who appointed Ms. Jankowicz to head the board as executive director? Were you aware of her history of partisan conduct prior to her appointment?**

Nina Jankowicz was chosen for her eminent qualifications and leadership in the field of online disinformation and malign foreign influence. She is a widely acknowledged expert on online disinformation who has testified multiple times before Congress as well as the UK and European Parliaments. From 2016-2017, under the auspices of the Fulbright program, Ms. Jankowicz served as an adviser to the Ukrainian Foreign Ministry. She worked closely with our Ukrainian allies to combat Russian disinformation meant to destabilize the Ukrainian government and jeopardize its international partnerships. Most recently, she was a Disinformation Fellow at the non-partisan Wilson Center.

**5. Has DHS conferred with any private social media company in the creation or operation of this board?**

The Board is an internal working group that does not have operational capacity. The creation of the Board was not discussed with any external entities prior to the public announcement.



.....  
(Original Signature of Member)

117TH CONGRESS  
2D SESSION

# H. R. \_\_\_\_

To direct the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security to identify, track, and share with homeland security stakeholders and the public information regarding misinformation, disinformation, and malinformation with national or homeland security implications, and for other purposes.

---

## IN THE HOUSE OF REPRESENTATIVES

Ms. CLARKE of New York introduced the following bill; which was referred to the Committee on

---

## A BILL

To direct the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security to identify, track, and share with homeland security stakeholders and the public information regarding misinformation, disinformation, and malinformation with national or homeland security implications, and for other purposes.

*Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,*

### SECTION 1. SHORT TITLE.

This Act may be cited as the “Strengthening Resilience Against Disinformation Act of 2022”.

**SEC. 2. DEFINITIONS OF MDM IN THE HOMELAND SECURITY ACT OF 2002.**

Section 2201 of the Homeland Security of 2002 (6 U.S.C. 652) is amended—

(1) by redesignating paragraphs (4), (5), and (6) as paragraphs (7), (8), and (9), respectively; and

(2) by inserting after paragraph (3) the following new paragraphs:

“(4) **DISINFORMATION.**—The term ‘disinformation’ means false information that is deliberately created to mislead, harm, or manipulate a person, social group, organization, or country.

“(5) **MALINFORMATION.**—The term ‘malinformation’ means information that is based on fact, but used out of context to mislead, harm, or manipulate.

“(6) **MISINFORMATION.**—The term ‘misinformation’ means information that is false, but not created or shared with the intention of causing harm.”.

**SEC. 3. RESPONSIBILITIES OF THE CISA DIRECTOR RELATING TO MISINFORMATION, DISINFORMATION, AND MALINFORMATION.**

(a) **IN GENERAL.**—Subsection (c) of section 2202 of the Homeland Security Act of 2002 (6 U.S.C. 652) is amended—

(1) in paragraph (13), by striking “and” after the semicolon;

(2) by redesignating paragraph (14) as paragraph (15); and

(3) by inserting after paragraph (13) the following new paragraph:

“(14) carry out activities to identify, track, and share with homeland security stakeholders and the public information regarding misinformation, disinformation, and malinformation, including by carrying out sections 2209(c)(13) and 2220D; and”.

(b) **NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER.** Subsection (c) of section 2209 of the Homeland Security Act of 2002 (6 U.S.C. 659) is amended—

(1) in subparagraph (11), by striking “and” after the semicolon;

(2) in paragraph (12), by striking the period at the end and inserting “; and”; and

(3) by adding at the end the following new paragraph:

“(13) maintaining capabilities to identify, track, and share with homeland security stakeholders and the public information regarding misinformation, disinformation, and malinformation that, either individually or in the aggregate, is likely to result in demonstrable harm to the national security interests of the United States, including undermining public confidence in democratic institutions or election integrity, or to homeland security, economic security, civil liberties, public health, emergency response, or public safety, or any combination thereof, for the purpose of enhancing the collective response to such misinformation, disinformation, and malinformation, including strengthening national security and promoting strong media literacy and digital resilience, including by carrying out activities in section 2220D.”.

**SEC. 4. RUMOR CONTROL PROGRAM OF THE DEPARTMENT OF  
HOMELAND SECURITY TO COUNTER MISINFORMATION,  
DISINFORMATION, AND MALINFORMATION.**

(a) IN GENERAL.—Subtitle A of title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.) is amended by adding at the end the following new section:

**“SEC. 2220D. RUMOR CONTROL PROGRAM TO COUNTER  
MISINFORMATION, DISINFORMATION, AND MALINFORMATION.**

“(a) ESTABLISHMENT.—There is within the center authorized pursuant to section 2209 a public-facing website, known as ‘Rumor Control’, to carry out sections 2202(c)(14) and 2209(c)(13).

“(b) FUNCTIONS.—In administering the Rumor Control website, the Director shall establish partnerships with relevant public and private sector stakeholders, including the following:



“(1) Technology companies that own or operate internet-enabled communications platforms commonly used to spread misinformation, disinformation, or malinformation.

“(2) Non-governmental and civil-society groups, including civil rights and civil liberties organizations, with relevant subject matter expertise or stakeholder relationships, to identify and respond to misinformation, disinformation, and malinformation, and ensure such response is designed to effectively reach and raise awareness among communities or demographics targeted by such content.

“(3) State, Local, Tribal, and territorial governmental agencies.

“(4) Relevant Federal agencies, including Sector Risk Management Agencies, as appropriate.

“(c) INFORMATION PROTECTIONS.—If in the course of carrying out this section personally identifiable information is received by the Agency, the Director shall ensure such information is protected from unauthorized use or disclosure in a manner consistent with the protection of personal information under the Cybersecurity and Information Sharing Act of 2015 (enacted as title I of division N of the Consolidated Appropriations Act, 2016 (Public Law 114–113)).”.

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by inserting after the item relating to section 2220C the following new item:

“Sec. 2220D. Rumor control program to counter misinformation, disinformation, and malinformation.”.

## **SEC. 5. REPORT.**

Not later than 180 days after the date of the enactment of this Act, and not later than 60 days after each regularly-scheduled general election for Federal office, the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report describing actions taken by the Director in furtherance of sections 2202(c)(14), 2209(c)(13), and 2220D of the Homeland Security Act of 2002, as amended and added by this Act, including

Release Authorized by Senator Grassley and Senator Hawley

specific details regarding the Agency's activities pursuant to subsection (b)(2) of such section 2220D, for the four-year period preceding each such election.

**(EXHIBIT E)**

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

----- Forwarded message -----

From: [REDACTED]  
Date: Tue, Jul 28, 2020 at 11:58 PM  
Subject: Trademark Infringement  
To: <[daytime@emmyonline.tv](mailto:daytime@emmyonline.tv)>

From: [REDACTED]  
Subject: Trademark Infringement  
[REDACTED]

Message Body:

I am emailing you to inform you that I came across a "gross" trademark violation. A YouTuber used the award, and portrayed it as the the Corona Virus. I find it beyond disrespectful, it is outrageous, my grandmother recently passed away from COVID-19.

I am attaching a link to what I saw.

<https://www.youtube.com/watch?v=MQ2xH7Z3584>

Sincerely,

[REDACTED]

**(EXHIBIT F)**

ARLINGTON GENERAL DISTRICT COURT - CIVIL ☒ General District Court ☐ Circuit Court  
☐ Juvenile and Domestic Relations District Court  
☐ Amended Protective Order ☐ Extension of Protective Order ☐ Conviction for Violation of Protective Order

**PETITIONER**

JANKOWICZ, NINA

LAST FIRST MIDDLE

And on behalf of minor family or household member(s):  
 (list each name and date of birth)

**PETITIONER'S DATE OF BIRTH**

3/10/1989

Other protected family or household members:  
 (list each name and date of birth)

V.

**RESPONDENT**

GOODMAN, JASON

LAST FIRST MIDDLE

252 7TH AVE #65

RESPONDENT'S ADDRESS

NEW YORK, NY 10001

**RESPONDENT IDENTIFIERS (IF KNOWN)**

RACE	SEX	BORN			HT.		WGT.	EYES	HAIR
W	M	MO.	DAY	YR.	FT.	IN.			
SSN									
DRIVER'S LICENSE NO.							STATE	EXP.	

☐ **CAUTION: Weapon Involved**

Distinguishing features:

**THE COURT FINDS** that it has jurisdiction over the parties and subject matter, that the Respondent was given reasonable notice and an opportunity to be heard, and that

- ☐ A warrant or petition has been issued charging the Respondent with a criminal offense resulting from the commission of an act of violence, force, or threat as defined in Va. Code § 19.2-152.7:1, **OR**  
☐ The Respondent has been convicted of  
☐ a criminal offense resulting from the commission of an act of violence, force, or threat as defined in Va. Code § 19.2-152.7:1.  
☐ a violation of a protective order pursuant to Va. Code § 18.2-60.4, **OR**

☒ A full hearing on the petition for a protective order has been held pursuant to Va. Code § 19.2-152.9(D), **OR**

☐ A hearing has been held pursuant to Va. Code § 19.2-152.10(B) on a motion to extend a protective order.

**THE COURT FURTHER FINDS** that the Petitioner and the Respondent

- ☐ cohabited more than 12 months ago but not within the past 12 months ☐ have never cohabited.

Accordingly, to protect the health and safety of the Petitioner and family or household members of the Petitioner,  
**THE COURT ORDERS** that:

☒ The Respondent shall not commit acts of violence, force, or threat or criminal offenses that may result in injury to person or property.

☒ The Respondent shall have no contact of any kind with the Petitioner

☐ except as follows:

☐ The Respondent shall have no contact of any kind with the family or household members of the Petitioner named above  
☐ except as follows:

☐ The Petitioner is granted possession of the companion animal described as

*directly, indirectly, by 3rd persons  
or by any means whatsoever*



Case No. GV23000138-00

☒ It is further ordered that

① Respondent remain, at least, 100 feet away from Petitioner and Petitioner's residence at all times.

② Respondent Prohibited from posting any social media regarding Petitioner

☐ Supplemental Sheet to Protective Order, Form DC-653, attached and incorporated by reference. Number of supplemental pages: .....

☒ The Respondent shall surrender, sell or transfer any firearm possessed by Respondent, within 24 hours after being served with this order, as follows:

- (a) surrender any such firearm to a designated local law-enforcement agency;
- (b) sell or transfer any such firearm to a dealer as defined in § 18.2-308.2; or
- (c) sell or transfer any such firearm to any person who is not prohibited by law from possessing a firearm.

☒ The Respondent shall, within 48 hours after being served with this order:

- (a) complete the attached certification form stating either that the Respondent does not possess any firearms or that all firearms possessed by the Respondent have been surrendered, sold or transferred; and
- (b) file the completed certification form with the clerk of the court that entered this order.

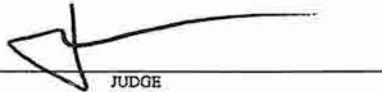
☐ Final judgment having been rendered on appeal from the juvenile and domestic relations district court, this matter is remanded to the jurisdiction of the juvenile and domestic relations district court in accordance with Virginia Code § 16.1-297.

THIS ORDER SHALL REMAIN IN FULL FORCE AND EFFECT UNTIL

02	13	2025	at 11:59 p.m.
MONTH	DAY	YEAR	

2/14/2023

DATE



JUDGE

#### WARNINGS TO RESPONDENT:

If Respondent violates the conditions of this order, Respondent may be sentenced to jail and/or ordered to pay a fine. This order will be entered into the Virginia Criminal Information Network. Either party may at any time file a motion with the court requesting a hearing to dissolve or modify this order; however, this Order remains in full force and effect unless and until dissolved or modified by the court. **Only the court can change this Order.**

**Federal Offenses:** Crossing state, territorial, or tribal boundaries to violate this order may result in federal imprisonment (18 U.S.C. § 2262). Federal law provides penalties for possessing, transporting, shipping or receiving any firearm or ammunition while subject to a qualifying protective order and under the circumstances specified in 18 U.S.C. § 922(g)(8).

**Full Faith and Credit:** This order shall be enforced, even without registration, by the courts of any state, the District of Columbia, and any U.S. Territory, and may be enforced on Tribal Lands (18 U.S.C. § 2265).

#### VIRGINIA FIREARMS PROHIBITIONS:

Pursuant to Code of Virginia § 18.2-308.1:4, Respondent shall not purchase, transport or possess any firearm while this order is in effect. For a period of 24 hours after being served with this order, Respondent may, however, continue to possess and transport a firearm possessed by Respondent at the time of service for the purposes of surrendering the firearm to a law-enforcement agency, or selling or transferring that firearm to a dealer as defined in § 18.2-308.2:2 or to any person who is not prohibited by law from possessing that firearm.

If Respondent has a concealed handgun permit, Respondent must immediately surrender that permit to the court issuing this order.

Case No. GY23000138-00

**RETURNS:** Each person was served according to law, as indicated below, unless not found.

<b>RESPONDENT:</b> NAME <u>Goodman, Jason</u> ADDRESS <u>252 7<sup>th</sup> Ave #65</u> <u>New York, NY 10001</u>	<b>PETITIONER: (See form DC-621, NON-DISCLOSURE ADDENDUM)</b> NAME <u>Jankowicz, Nina</u>
<input checked="" type="checkbox"/> <b>PERSONAL SERVICE</b>	<input checked="" type="checkbox"/> <b>PERSONAL SERVICE</b>
<input type="checkbox"/> <b>NOT FOUND</b>	<input type="checkbox"/> <b>NOT FOUND</b>
<u>Deputy Y. Lopez S1317</u> SERVING OFFICER for <u>Sheriff Jose Quiroz</u> <u>02/14/2023</u> <u>1505 hours</u> DATE AND TIME	<u>Deputy Y. Lopez S1317</u> SERVING OFFICER for <u>Sheriff Jose Quiroz</u> <u>02/14/2023</u> <u>1500 hours</u> DATE AND TIME
<b>RESPONDENT'S DESCRIPTION (for VCIN entry):</b> RACE <u>W</u> SEX <u>M</u> DOB: <u>04/07/1972</u> HGT <u>5'7"</u> WGT <u>150</u> EYES <u>Green</u> HAIR <u>Brown</u> SSN <u>089-50-7157</u> Tel. No. <u>347-380-6998</u> Relationship to Petitioner/Plaintiff <u>none</u> Distinguishing features <u>none</u>	<input type="checkbox"/> <b>Copy delivered to:</b>  by _____ TITLE _____ SIGNATURE _____

**DEFINITIONS:**

"Family or household member" means (i) the person's spouse, whether or not he or she resides in the same home with the person, (ii) the person's former spouse, whether or not he or she resides in the same home with the person, (iii) the person's parents, stepparents, children, stepchildren, brothers, sisters, half-brothers, half-sisters, grandparents and grandchildren regardless of whether such persons reside in the same home with the person, (iv) the person's mother-in-law, father-in-law, sons-in-law, daughters-in-law, brothers-in-law and sisters-in-law who reside in the same home with the person, or (v) any individual who has a child in common with the defendant, whether or not the person and that individual have been married or have resided together at any time, or (vi) any individual who cohabits or who, within the previous twelve (12) months, cohabitated with the person, and any children of either of them residing in the same home with the person.

"Act of violence, force, or threat" means any act involving violence, force, or threat that results in bodily injury or places one in reasonable apprehension of death, sexual assault, or bodily injury. Such act includes, but is not limited to, any forceful detention, stalking, criminal sexual assault in violation of Article 7 (§ 18.2-61 et. seq.) of Chapter 4 of Title 18.2, or any criminal offense that results in bodily injury or places one in reasonable apprehension of death, sexual assault, or bodily injury.